OPEN ACCESS
Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

Digitalization and Industrial Revolution 4 (IR4) Technologies

Rajesh D Savio[1*]

[1]Lead – OE & Compliance Group, Jazan Complex Projects Department, Saudi Aramco

DOI: 10.36348/sjet.2022.v07i07.002 | **Received:** 29.06.2022 | **Accepted:** 01.08.2022 | **Published:** 10.08.2022

***Corresponding author:** Rajesh D Savio
Lead – OE & Compliance Group, Jazan Complex Projects Department, Saudi Aramco

Abstract

With the advent of the Industrial Revolution 4 (IR4), many new challenges have emerged. One such issue is privacy and security. Millions of devices are now connected to the internet, and there is no concrete way to ensure that the user has authority (or) control over its data. This study addresses this challenge by drawing a theoretical framework for IoT software that can provide mathematical proof to the user regarding the privacy of the data. Such a certification would ensure that the data remains confidential as well as it will accelerate the rate of adoption of IoT technologies.

Keywords: Industrial Revolution 4, privacy and security, IoT technologies, Digitalization.

INTRODUCTION

The fourth generation of the industrial revolution has swept outwards and has the ability to transform every human sphere. Such a revolution would radically redefine human interaction ranging from industries to societal patterns [1]. The focus of IR4 is on building consciousness in the machines that are also called Artificial Intelligence (AI), editing the genes of human bodies, emphasis on robotics to do the manual work, etc. Developing such technology has posed some new problems as well. Consider one of the most important implications of IR4 that is the concept of smart homes. This would connect every device in the homes of the users with artificial intelligence that would have the ability to work by itself. However, this would pose a challenge to the privacy of users. The issue of data privacy is the most significant challenge in IR4 [2]. This is the problem that this study would be targeting.

The current solutions offered to protect the data of the users are inadequate. This is evident from the fact that many data privacy software has been developed over the years, such as Schrems II; however, the issue still persists. With a greater reliance on technology, there is a clear need for the users to have data privacy software that can ensure the long- term privacy of the users and make the data protected from outside interference. The solution of formulating a new certification program for data privacy in the domain of IoT is quite apparent. This would ensure that no type of hacker can intervene in the customer's connected device. Regardless of the fact that every device in the user's home is connected through the mobile phone, this certification would ensure that there is no security breach. This type of solution would be a breakthrough in IoT and make the adoption of IoT faster.

Henceforth, the study would be structured around formulating such an IoT certification. It would first bring into light different academic papers regarding the state problem. Building on this, the study would develop an implementation plan. This plan would serve as a litmus test of the certification that is being proposed. The later part of the study will discuss the evaluation or testing of the solution and how the proposed solution is better than the ones already existing.

Related Work

Existing Solution

In 2020, there were between 50-100 billion devices that were connected to the internet [3]. This has made the debate of data privacy at the helm criticizing the role of government and private corporations in invading and spying on the privacy of the users. The study states the development of Medium Access Control or MAC as an existing technology to address the need for data privacy. MAC is a sublayer that is responsible for sending and receiving data between different devices [4]. Through this technology, the data communication path can be anonymized, ensuring that the data cannot be traced back to its original source.

However, relying on MAC for complete data security is not an advisable task as it is particularly easy to construct profiles for the knowledge extraction of a single user.

In addition, it must also be considered that there are different methods accepted in the fourth industrial world to protect IoT data. This is discussed in length as this type of protection must include six main steps [5]. The first step is that the organizations must maintain visibility over the whole process of data flow. This would include adding monitoring devices to see and detect if there is an outside intervention in the data. The second step is based on the categorization of data. This means that organizations should not adopt a monolithic approach to data privacy. It should assign and prioritize what data is critical and contains sensitive information. Once this step is achieved, it can make the job of data privacy easier as there would be a lesser volume of data after the screening process. The third and most important step is the encryption of data. This is also discussed in detail [6]. As per these researchers, the process of encryption is absolutely important as it converts the data, which is in understandable form, into encryption. Furthermore, the process also entails designing the security. This translates to devising a data protection strategy and deciding on security protocols. This step would lead towards the security of the components. A security certification scheme such as PSA Certification is quite relevant to this step. PSA certification works from chip hardware to the cloud, ensuring that each and every step in the data chain is protected [7]. In other words, such a type of certification is highly credible and proof to customers that their data will not be mingled by any other external source. The last step in the securitization of IoT is deciding on a governance program. Some basics of the governance program are getting a consensus on log management, strong password policies, and a program for patch management.

Talking about security certification for IoT data, another existing solution exists in the name of (IoT) Cybersecurity Certification. As highlighted by [8], CTIA certification has existed for more than 30 years in the market, and during this time, it has been successful in developing an industry standard. This ensures that there is a global certification program for IoT devices that are connected to cellular networks. When translated into practical examples, the certification is empowering in the domains like real estate, fleet tracking, and food storage. In addition to these certifications, there is also Certified Internet of Things Security Practitioner (CIOTSP). The objective of this certification program is not to provide software or develop a solution but rather to upskill the network team. The program aims to build the foundational skills of the development team that can transform individuals into IoT security experts. These individuals can then tailor the security programs based on the needs and requirements of their respective organizations.

Areas of Improvement

On the contrary, it must also be also noted that each of the existing certification programs that are discussed has its own problems. The first major problem is that neither of the certifications is wholesome. For instance, almost all of the regular patches have a weak update mechanism. This is because the process of securitization of IoT data is continuous [9]. It is always evolving as hackers develop more sophisticated technology to break into the systems. The study [10] has also highlighted one of the most basic issues in security management of IoT that is heterogeneity. As per the authors, this is a concept that requires different devices to be incorporated legitimately or illegitimately within the IoT framework. This makes the issue of security among the most important as there is a need for connecting multiple devices into one centralized hub. The study also states the importance of sensors. Sensors form the core of IoT infrastructure as they are composed of the initial layer of IoT infrastructure called as perception or sensing layer. The role of sensors is of incredible importance as it detects signals and establishes communication between different devices. However, when formulating the security network, the intriguing nature of these sensors must be understood in both the single devices as well as in the networks. The issue of security becomes more complex as more and more devices come into connection with the overall IoT infrastructure. And hence, as the devices assimilate into IoT, managing security and ensuring the privacy of the data becomes more legitimate.

Implementation

As discussed above, the solution that is proposed is related to developing a security certification for IoT devices. As more and more devices are being connected to IoT infrastructure, there is a need for devising a global security standard that can be adopted industry-wide. This solution is based on mathematical rules as security can be proved rigorously with well based mathematic principles. The current computer world has never been conceived in this way, and all the protocols are insufficiently developed so that the security breaches and attacks are made possible, which is not the case should the security be designed from the ground up with strict measures. As of now, there is little to no control over the data management that is sent to the cloud by the users. This makes security breaches very possible and alienates the users. However, with our specified certification program, the software would empower the users as they can have complete control and monitoring authority over the data that is stored on the cloud. So, in other words, this type of technology cannot be developed unless it gets the attention of the relevant stakeholders, including the government and the private sector. Under this paradigm, the data will be

completely privatized, meaning that the users control different operations like the party that can store the data, pass the data, or perform different kinds of operations. To this end, there is a need for formulating a technical framework based on rigorous mathematical principles. As stated, modern software is able to carry proof together with computation to exhibit the properties of computation and data [11]. In this way, it will be possible to gain control over one's own data or, more generally, about the flow, privacy, and transmission of data. It has to be a technology that can prove that the data is protected from outside or external interference and that the user has complete authority over the user's own data.

In addition, the technology is based on two components. The first one deals with the technical aspect. This is where the rigorous mathematical calculations take place and ensure that there is no violation of your confidential data. This also means that there is a cross-communication of proofs between the machines to verify what users want or what practices need to be adopted. The other part is concerned with obtaining certification. This certification would ensure that there are no back doors or mechanisms to circumvent the verified information. Other than these components, there are basic components of the software that are discussed below.

Specification language

Allows users to define the capabilities and properties of their system using a human-readable formal description language.

Extractor

The specification is processed by the extractor to produce (A) an executable transcription for consumption by the program executor and (B) input for the solver.

Solver

Allows the validation of requests against a given specification in order to provide formal proof of their correctness.

Program Execution

Allows the direct execution of programs and workflows derived from the specification in interaction with the client system.

Web Client

Allows users to create specifications, access the solver, and control program execution through an intuitive graphical user interface.

API

Allows machine agents to define specifications, access the solver, and control program execution.

This vision is in complete contrast to the existing security solutions offered in IoT infrastructure. For instance, companies like Google or Meta are built on the principle of using or selling your data in a way that the user has no information about it. So, your private and confidential information is at the mercy of these corporations whose business model is to sell your data. Furthermore, this certification ensures and guides the error-free operation of distributed systems. Provided with declarative specifications of each constituent systems data type and capability, the security certification facilitates their interaction following logical proof of its formal correctness. It orchestrates this process through a workflow management system (WFMS) that ensures a secure, safe, and reliable operation of the distributed system in question. The software declarative specification language lets service providers give formal descriptions of the capabilities of their systems. The software then (A) validates the integrity of all of its client's connections against their service specification and (B) directly enacts action schemas derived from the specification by controlling communication with the client application. The WFMS provides an infrastructure that enables the orchestration of complex workflows through the combination of the above-mentioned capabilities in the composition, execution, and monitoring of interdependent tasks. The software, therefore, provides vital capabilities in the operation of complex and heterogeneous distributed systems. Its design is based on well-founded theory so that it is least susceptible to malware and bugs itself (see Section III: Implementation). Requiring clients to provide formal and correct specifications during the design or enlistment of service for the certification ensures that edge cases and limitations are correctly handled. In the continued operation of services, compliance with the specification is ensured, even given unannounced changes in communication protocols or the dynamic addition or removal of distinct service providers.

Evaluation

Currently, there is no such product that operates on this logic. The new products work on functional programming dependent type and proof-carrying codes. As stated, a proof-carrying code is a mechanism that gives the authority to the host system to acknowledge the applications through a consented proof that comes along with the application's executable code [12]. This type of technology is completely different from the one that is offered right now. In today's world, the web is much more open and, as a result, more vulnerable to an external threat. This puts the challenge of security at the forefront and exposes the users to outside attacks. However, in the solution software that we have proposed, such kind of external threat would be extremely difficult to manage. It must also be noted that the solution that we have formulated does not make the threat inevitable but is surely very difficult. This is an ideal system for protecting IoT infrastructure.

In addition, when it comes to testing the product, there are two types of tests such as module tests and system tests that are both applicable for testing the solution. The certification program that we have designed can be passed through both the tests, and its validity can be verified. These tests serve as a baseline for the authenticity of the product. However, there is space for improvement by introducing another type of test. Another type of test is known as Adaptive Random Testing. As discussed by Chen *et al.*, [13], Adaptive Random Testing is used for generating random data to check the vulnerability of security software. Unlike other testing systems, Adaptive Random Testing has more potential to check the severity of the program and ensure that there is no loophole in the programming. It must also be noted that the mathematical proofs are already secure, but there is a chance that they can be willingly or unwillingly tempted to technical incompleteness. Hence, there is room for adding additional testing, which is Adaptive Random Testing.

The situation as it is now, IoT has penetrated into homes and industries. This puts the privacy and security of each and every one of us at stake. For instance, if someone buys an IoT product and connects it to their house, this data is very easy to invade and share. The companies making these products do not have a high degree of security, and the risk is transferred to the users. Users enter their details and connect the machine, and as a result, the hackers can penetrate into their houses. The housing data is very easily accessible, and it is not only for the hackers but for the entire ecosystem ranging from manufacturers to IT companies to governments. However, within our certification program, the users will have control over the data rights and privacy. This would be achieved through a rigorous mathematically based technology that is constructed for ensuring maximum safety, privacy, and control of data. This solution is not only viable for the users, but it has even great importance for commercial users as well. This is because the data from the companies and private sector is of utmost importance and needs to be protected at all costs. Yet, with the current state of technology, this privacy is compromised, and everything now is based on the trust and benevolence of multinational companies. This is not exactly a technical solution, and the world deserves more, especially in the age of IR4. Furthermore, if any company offers a data service through hackers or servers, the data get abused. This can have a very negative implication for companies. Hence, this solution serves as the resurrection and protection of the commercial class by ensuring that their data is highly protected and impenetrable.

Challenges

In addition to the evaluation, there are certain challenges that may arise during the development of such a security certification software. They are listed below:

1) The design of the specification language requires a trade-off between expressiveness and its capacity to be automatically provable. High expressiveness is generally desirable in order to support the exact specification of a wide range of system properties. Still, the constructs necessary for that can bring about decision problems in the validation of requests that require manual oversight. Here, a compromise must be found in order to limit the set of problems for which proof hints have to be given by a human user and which are highly improbable to occur in an actual live system.
2) Primitives for the language need to be carefully selected. Especially primitives that capture concurrency, parallelism, and distribution require careful consideration (e.g., SessionTypes, LTL).
3) The system can only play out its full capacities if it provides high usability to software engineers that operate it. An intuitive and unambiguous user interface will enable users to retain an overview of their description of a highly complex and abstract system.
4) The solver needs to perform in real-time for complex real-world problems. This requires an implementation that opts for high performance. Our approach for providing this is (A) to use functional programming, (B) to compile the human-readable specification language to simpler, processing-oriented languages (e.g., by applying Second- Order Quantifier Elimination) (C) to base the most simplified language on Constraint Handling Rules 1 and (D) to implement an industrial-strength solver using highly parallelized processing capabilities of modern GPUs (cf. Zaki, Fruhwirth, and Geller n.d. ¨ for an academical proof-of-concept of this approach).
5) Our clients will require assurances of our claim to provide them with integrity and security of their operation. Therefore, will utilize the Coq Proof Assistant 2 to show the consistency and validity of the specification language and the descriptions expressed in it, as well as the correctness of all transformations derived from them and their use in our solver.

CONCLUSION

The problem that was highlighted in this study relates to security. In the age of IoT, the current web has failed to adapt itself to the technology. So, the issues of privacy and security are largely unaddressed, and there is a clear need for certification security software that can ensure that the user's household data is protected. Such type of a solution can also accelerate the large-scale adoption of IoT services. To this end, we have formulated a rigorous mathematically-proof technology that secures the data services from outside

attacks. This solution is better than the existing technologies as the protocols specify the services in a formal way, and the implementation proofs that this specification gets fulfilled and the client of these services can negotiate with the proofs that everything they get is already verified and proofed. So, in other words, this certification instills a mathematical consciousness among the devices. The current web is wild as anyone can intervene in anyone's data without being identified. This is because www was created over 50 years ago, and we are still using obsolete technology. However, our certification program is an evolution to www as it makes the services securer. This certification has a technological sophistication, and the ones who want to acquire it would have to purchase this software for a fee. For instance, if a company has a service and this service accesses another service with lesser security guarantees, then this service which is written in the highest security level, then gets downgraded to lower the security level of the service it accesses because security can be threatened by the lower security service. Hence, this type of solution is not only for IoT or companies or individual entities, but it touches basic human rights that have thus far not been envisioned. The software opens a new chapter in the history of humanity and computing, and there should be a global political consensus on the need to update the security certification programs.

REFERENCES

1. Ismail, A. A., & Hassan, R. (2019). Technical competencies in digital technology towards industrial revolution 4.0. *Journal of Technical Education and Training*, *11*(3).
2. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of things Journal*, *5*(5), 3758-3773.
3. Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT Professional*, *17*(3), 32-39.
4. Taneja, K., Taneja, H., & Kumar, R. (2018). Multi-channel medium access control protocols: review and comparison. *Journal of Information and Optimization Sciences*, *39*(1), 239-247.
5. Pratt, M. K. (2021). Fortify security with IoT data protection strategies. *Internet of Things Agenda*. Retrieved from https://internetofthingsagenda.techtarget.com/tip/Fortify-security-with-IoT-data-protection-strategies.
6. Yazdeen, A. A., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021). FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. *Qubahan Academic Journal*, *1*(2), 8-16.
7. PSA Certified. (2022). Security Certification for Chip Vendors. Retrieved from https://www.psacertified.org/getting-certified/silicon-vendor/overview/. 2022
8. IoT Network Certified. (2022). Powering the future of connectivity. Retrieved from https://iotnetworkcertified.com/.
9. Thales. (2021). IOT SECURITY ISSUES IN 2021: A BUSINESS PERSPECTIVE. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats#:~:text=Insufficient%20data%20protection%20(communication%20and,used%20to%20access%20confidential%20data.
10. Hasan, N., Chamoli, A., & Alam, M. (2020). Privacy challenges and their solutions in IoT. In *Internet of things (IoT)* (pp. 219-231). Springer, Cham.
11. Hu, L., Wen, H., Wu, B., Pan, F., Liao, R. F., Song, H., Tang, J., & Wang, X. (2017). Cooperative jamming for physical layer security enhancement in Internet of Things. *IEEE Internet of Things Journal*, *5*(1), 219-228.
12. Venugopalan, V., & Patterson, C. D. (2018). Surveying the hardware trojan threat landscape for the internet-of-things. *Journal of Hardware and Systems Security*, *2*(2), 131-141.
13. Chen, T., Leung, H., & Mak, I. (2004). Adaptive Random Testing, *Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making*, p. 320-329. Available: 10.1007/978-3-540-30502-6_23.