Papers

1- El Mamy SIDI BOUBACAR, Hassen Gharbi and Abderrazak Jemai, **A Detailed Survey of Blockchain and Its Applications**

Adresses mail { elmamy.sidiboubecar@etudiant-fst.utm.tn , hassen.gharbi@ensi-uma.tn, Abderrazak.Jemai@insat.rnu.tn }

Abstract - Blockchain is being termed as the fifth disruptive innovation in computing and has numerous benefits such as decentralization, persistency, anonymity and auditability. There is a wide spectrum of blockchain applications ranging from financial services, Internet of Things to public and social services. In simplest words, it is a distributed ledger of records that is immutable and verifiable. Since its advent in 2008, blockchain as a concept has been used in various ways. The largest impact or application is seen as a multitude of cryptocurrencies that have sprung up. However, with time, it has become clear that blockchain as a technology is likely to have an impact much wider than just the cryptocurrency domain and much deeper than simple distributed ledger storage. This detailed survey intends to bring together all the key developments so far in terms of putting blockchain to practice. This paper will explore the various domains where blockchain has had an impact and where future implementations may be expected.

2- Ihsen Alouani, " **Internet of Things: Emerging Security Challenges and Perspectives**"

Email ihsen.alouani@uphf.fr

Abstract: The Internet of Things (IoT) has radically trans-formed several real-life domains thereby improving human life quality. It represents one of the fastest developing fields in the his-tory of computing, with an estimated 50 billion devices by the end of 2020. Billions of connected devices are able to communicate with more and more autonomy enhanced with embedded machine learning technology. While this technology has promising impact on our lives, IoT has inherent vulnerabilities imposed by the design constraints and the time to market pressure. In fact, the low power budget and the by-construction limited resources of IoT devices shrink the security-dedicated budget and resources. Moreover, the race to the emerging IoT market makes security second-rank parameter and an afterthought in the design process. More recently, the development of machine learning and deep learning (ML/DL) techniques has been deployed in various IoT use cases such as intelligent transportation systems (ITS),access control, speech recognition, medical applications, etc. This association of embedded intelligence along with IoT has brought even higher risks since ML has its own inherent vulnerabilities such as adversarial attacks. In this paper, we draw a landscape of emerging risks facing the development of safe and secure IoTs, along with a perspective on potential defense strategies.

3- Rim ZARROUK and Abderrazak JEMAI, **Embedded Particle Swarm Optimization for smart factory Scheduling (Industries 4.0 era)**

Adresses mail { rima.zarrouk@gmail.com, Abderrazak.Jemai@insat.rnu.tn }

Abstract—Embedded systems have become an essential part of our lives, mainly due to the Industry 4.0 birth. However, the power consumption of these devices is one of their most important drawbacks. It has been proven that an efficient use of the CPU of the device also improves its energy performance. The use of the Particle Swarm Optimization (PSO) over an

embedded environment achieve many resources problems. In this paper, an embedded two-level PSO (E2L-PSO) for intelligent real-time simulation is introduced. An automatic adaptation of the asynchronous embedded two-level PSO algorithm to CPU needs is done. The flexible job shop scheduling problem (FJSP) is selected to solve due to its importance in the Industries 4.0 era. An analyze of the run time performance on handling E2L-PSO over a Raspberry Pi B+ card was done. By the experimental study, such optimization permits to decrease the CPU time consumption by 10% to 70% according to CPU reduction needed (soft, medium or hard reduction).

4- Nicolas Fleury, Theo Debrunquez and Ihsen Alouani "PDF-Malware: An Overview on Threats, Detection and Evasion Attacks"

Abstract: In the recent years, Portable Document Format, commonly known as PDF, has become a democratized standard for document exchange and dissemination. This trend has been due to its characteristics such as its flexibility and portability across platforms. The widespread use of PDF has installed a false impression of inherent safety among benign users. However, the characteristics of PDF motivated hackers to exploit various types of vulnerabilities, overcome security safeguards, thereby making the PDF format one of the most efficient malicious code attack vectors. Therefore, efficiently detecting malicious PDF files is crucial for information security. Several analysis techniques have been proposed in the literature, be it static or dynamic, to extract the main features that allow the discrimination of malware files from benign ones. Since classical analysis techniques may be limited in case of zero-days, machine-learning based techniques have emerged recently as an automatic PDF-malware detection method that is able to generalize from a set of training samples. These techniques are themselves facing the challenge of evasion attacks where a malicious PDF is transformed to look like benign. In this work, we give an overview on the PDF-malware detection problem. We give a perspective on the new challenges and emerging solutions