**COVERT WIRELESS COMMUNICATION IN IOT NETWORK: FROM AWGN CHANNEL TO THZ BAND**

**[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao:** Fog/edge computing has been proposed to be integrated with Internet-of-Things (IoT) to enable computing services devices deployed at network edge, aiming to improve the user’s experience and resilience of the services in case of failures. With the advantage of distributed architecture and close to endusers, fog/edge computing can provide faster response and greater quality of service for IoT applications. Thus, fog/edge computing based IoT becomes future infrastructure on IoT development. To develop fog/edge computing-based IoT infrastructure, the architecture, enabling techniques, and issues related to IoT should be investigated first, and then the integration of fog/edge computing and IoT should be explored. To this end, this paper conducts a comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues, and present the integration of fog/edge computing and IoT, and applications. Particularly, this paper first explores the relationship between Cyber-Physical Systems (CPS) and IoT, both of which play important roles in realizing an intelligent cyber physical world. Then, existing architectures, enabling technologies, and security and privacy issues in IoT are presented to enhance the understanding of the state of the art IoT development. To investigate the fog/edge computing-based IoT, this paper also investigate the relationship between IoT and fog/edge computing, and discuss issues in fog/edge computing-based IoT. Finally, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in rea lworld applications.

**Summary:** In this paper, a comprehensive review of IoT has been presented, including architectures, enabling technologies, and security and privacy issues, as well as the integration of fog/edge computing and IoT to support diverse applications. Particularly, the relationship and difference between IoT and CPS has been clarified at the outset. Possible architectures for IoT have been discussed, including the traditional three-layer architecture and the SoA-based four-layer architecture.

**[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino**,**:** Social Internet of Things (SIoT) is a new paradigm where Internet of Things (IoT) merges with social networks, allowing people and devices to interact, and facilitating information sharing. However, security and privacy issues are a great challenge for IoT but they are also enabling factors to create a “trust ecosystem.” In fact, the intrinsic vulnerabilities of IoT devices, with limited resources and heterogeneous technologies, together with the lack of specifically designed IoT standards, represent a fertile ground for the expansion of specific cyber threats. In this paper, we try to bring order on the IoT security panorama providing a taxonomic analysis from the perspective of the three main key layers of the IoT system model: 1) perception; 2) transportation; and 3) application levels. As a result of the analysis, we will highlight the most critical issues with the aimof guiding future research directions.

**Summary:** Here, it is shown that that IoT system model has many security issues among which threats that can exploit some possible weaknesses. For these reasons, it is necessary to appropriately enforce trust management and security in the IoT world starting from the characterization of the different threats related to each specific level of the general IoT system model.

**[3] Y. Lu and L. D. Xu:** As an emerging technology, the Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, information, and data. The development of IoT is still in its infancy and many directly related issues need to be solved. IoT is a unified concept of embedding everything. IoT has a great chance to make the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. But, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. This article systematically reviews IoT cyber security. The key factors of the paradigm are the protection and integration of heterogeneous smart devices and information communication technologies (ICT). Our review applies to people interested in cyber security of IoT, such as the current research of IoT cyber security, IoT cyber security architecture and taxonomy, key enabling countermeasures and strategies, major applications in industries, research trends and challenges

**Summary:** we have vigorously surveyed the important aspects of IoT cyber security, specifically, the state-of-the-art of the current position and potential future directions, the major

Counter measures against IoT attacks, and the applications in industries. In addition, we introduced and discussed a possible four-layered IoT cyber security infrastructure and a taxonomy of attacks on IoT cyber security.

**[4] Y. Miao, X. Liu, K. R. Choo, R. H. Deng, H. Wu, and H. Li:** Cloud-assisted Internet of Things (IoT) is increasingly prevalent in our society, for example in home and office environment; hence, it is also known as Cloud-assisted Internet of Everything (IoE). While in such a setup, data can be easily shared and disseminated (e.g., between a device such as Amazon Echo and the cloud such as Amazon AWS), there are potential security considerations that need to be addressed. Thus, a number of security solutions have been proposed. For example, Searchable Encryption (SE) has been extensively studied due to its capability to facilitate searching of encrypted data. However, threat models in most existing SE solutions rarely consider the malicious data owner and semi-trusted cloud server at the same time, particularly in dynamic applications. In a real-world deployment, disputes between above two parties may arise as either party will accuse the other of some misbehavior. Furthermore, efficient fullupdate operations (e.g., data modification, data insertion, data deletion) are not typically supported in the cloud-assisted IoE deployment. Therefore, in this paper, we present a Fair and Dynamic Data Sharing Framework (FairDynDSF) in the multi owner setting. Using FairDynDSF, one can check the correctness of search results, achieve fair arbitration, multi-keyword search, and dynamic update. We also prove that FairDynDSF is secure against inside keyword guessing attack and demonstrate its efficiency by evaluating its performance using various datasets.

**Summary:** In thispaper, we proposed an efficient and practical FairDynDSF, which supports result verification, dispute arbitration, dynamic update, decryption authorization and expressive keyword search simultaneously. In addition, FairDynDSF is also designed to be resilient to data corruption attacks and sufficiently lightweight for deployment on resource-constrained IoT devices. The formal security analysis showed that FairDynDSF is secure against inside KGAs, and the empirical examination using various datasets demonstrated that FairDynDSF is practical and scalable in practice.

**[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha:** Covert communication, also known as low probability of detection (LPD) communication, prevents the adversary from knowing that a communication is taking place. Recent work has demonstrated that, in a three-party scenario with a transmitter (Alice), intended recipient (Bob), and adversary (Warden Willie), the maximum number of bits that can be transmitted reliably from Alice to Bob without detection by Willie, when additive white Gaussian noise (AWGN) channels exist between all parties, is on the order of the square root of the number of channel uses. In this paper, we begin consideration of network scenarios by studying the case where there are additional “friendly” nodes present in the environment that can produce artificial noise to aid in hiding the communication. We establish achievability results by considering constructions where the system node closest to the warden produces artificial noise and demonstrate a significant improvement in the throughput achieved covertly, without requiring close coordination between Alice and the noise-generating node. Conversely, under mild restrictions on the communication strategy, we demonstrate no higher covert throughput is possible. Extensions to the consideration of the achievable covert throughput when multiple wardens randomly located in the environment collaborate to attempt detection of the transmitter are also considered.

**Summary**: In this paper, first step in establishing low probability of detection (LPD) communications in a network scenario. We established that Alice can transmit O(mγ/2√ n) bits reliably to the desired recipient Bob in n channel uses without detection by an adversary Willie if randomly distributed system nodes of density m are available to aid in jamming Willie; conversely, no higher covert rate is possible.

.