The conventional form of electric grid, which caters to the electricity needs of a mammoth population, is considered to be very successful and reliable. It consists of four major components: generation of electric energy in different manners, transmitting it via a very high voltage infrastructure, distribution for consumption and consumption for industrial and residential purposes. Some of the challenges faced by the conventional grid include maintaining balance between supply and demand, fulfilling peak demand and energy and cost saving for both consumers and providers. To address these challenges, the smart grid concept has evolved. The smart grid uses communications and information technologies to provide better situational awareness to utilities regarding the state of the grid. Using intelligent devices, smart grid has shown that the peak demand can be flattened and future demand can be predicted resulting in drastic cost reduction for both power generation and consumption. However, smart grid also poses a series of new security challenges, among others, that require novel approaches to the field of cyber security. Existing security approaches have proven to be insufficient to tackle the security threats as the size and complexity of grid networks provide numerous potential entry points. The most common mechanism to penetrate a trusted perimeter of devices is through a network-based attack vector. Exploiting poorly configured firewalls for misconfigured inbound and faulty outbound rules is a common entry point, enabling an adversary to insert a malicious payload onto the control system. Secondly, an employee or legitimate user who is authorized to access system resources can perform actions that are difficult to detect and prevent. Privileged insiders also have intimate knowledge of the deployed defence mechanisms, which they can often easily circumvent. Also, an attacker can preinstall malicious codes into a device prior to shipment to a target location, called supply chain attacks.

The attacks mentioned above are not exhaustive with a never-ending list. Out of the many countermeasures suggested by various researchers to maintain the security of smart grid, developing a secure communication architecture seems to be an important one. Designing a highly resilient communication architecture for a smart grid is critical to mitigate attacks while achieving high level availability. A secure communication architecture involves secure key management, network topology, packet routing and forwarding protocol and data secrecy and authenticity. Key management is a fundamental approach for information security. Shared secret keys or authentic public keys can be used to achieve secrecy and authenticity for communication. Authenticity is especially important to verify the origin which in turn is key for access control. The network topology can also have an impact on the robustness against attacks. One simplest way to prevent communication is by attacking the routing protocol. By compromising a single router and by injecting bogus routes, all communication in the entire network can come to a standstill. Thus, a secure routing protocol is essential on top of a network topology. Securing individual routers and detecting malicious behaviours is also required to ensure network security. Similarly, secure broadcasting for price dissemination is important, because an adversary could inject a negative cost and cause electricity utilization to spike when numerous devices simultaneously turn on to take advantage of the low price. Data secrecy and authenticity are also important to prevent data from being accessed by unauthenticated user. Secrecy prevents an eavesdropper from learning the data content, while enables the receiver to verify that the data indeed originated from the sender, thus preventing an attacker from altering the data. Given all the above mechanisms, enabling communication under Denial of Service (DoS) attacks is crucial to perform network management operations to defend against the attack.

The research paper shows that cyber-physical system security approaches consider physical as well as system aspects in more detail than the traditional security and cryptographic approaches. It demands additional security requirements, such as continuity of power delivery and accuracy of dynamic pricing, introduced by the physical system. The paper also describes about various fields in detail that offer exciting research challenges related to cyber-physical system security. It would have been better had the authors tried to develop different types of attacks on the smart grid, analysing their impacts. This could then might have been followed by a detailed description of potential solutions for the attacks. Apart from the system theoretic and cyber physical approaches mentioned in the paper, inclusion of game-theoretic scheduling model used in a smart grid management would have made it more interesting. The paper describes a couple of security approaches as mentioned above but lacks in backing them up with real data. We can simulate the mentioned approaches on real-world smart grids with a visualization of results that could have help in proving the theoretical approaches as more robust and ready-to-apply. We can also describe how the security approaches mentioned in the paper can benefit both electricity consumers and providers and help in achieving the main purpose of cost and energy. Conventional message authentication schemes and the physical layer authentication mechanisms can be combined to achieve fast authentication while minimising the packet transmission overhead. This can help in providing real-time control over the smart grid.