Hindustan

Institute of Technology & Science.

Department: **Information Technology**

NETWORKS AND INFORMATION SECURITY (ITB4317)

Assignment -1

Submitted To:

DR MEENAKSHI N

(ASSISTANT PROFESSOR)

Submitted By:

Vitul Chauhan 18132023/IT/6A-Gen

Context: *According to Union Ministry of Power, "state-sponsored" Chinese hacker groups targeted various Indian power centres including Mumbai. The Ministry also said that these groups have been thwarted after government cyber agencies warned it about their activities. Even the New York Times reported that the Mumbai power outage in October 2020 was part of a coordinated cyberattack by China*

- ⇨ A smart grid communication security solution requires a holistic approach including traditional schemes such as public key infrastructure technology, trusted computing elements, authentication mechanisms based on industry standards

Introduction:

A smart grid is a new form of electricity network with high fidelity power-flow control, self-healing, and energy reliability and energy security using digital communications and control technology. To upgrade an existing power grid into a smart grid, it requires significant dependence on intelligent and secure communication infrastructures. It requires security frameworks for distributed communications, pervasive computing and sensing technologies in smart grid. However, as many of the communication technologies currently recommended to use by a smart grid is vulnerable in cyber security, it could lead to unreliable system operations, causing unnecessary expenditure, even consequential disaster to both utilities and consumers. In this paper, we summarize the cyber security requirements and the possible vulnerabilities in smart grid communications and survey the current solutions on cyber security for smart grid communications

Requirements: *Meanwhile, the higher degree of connectivity should have corresponding sophisticated security protocols to deal with the cyber security vulnerabilities and breaches. Some security protocols adopted by different layers in communication networks with the specific security requirements,*

Analysis:

POWER industry is integrating the electrical distribution system with communication networks to form a two directional power and information flow infrastructure, which is called a smart grid [1].

Compared with regular enterprise network systems, smart grid communication systems have different goals, objectives and assumptions concerning what need to be protected in cyber security.

It surveys the existing solutions for cyber security in smart grid communications.

Trust management systems, based on public key infrastructure (PKI) technology, could be customized for smart grid operators, easing the burden of providing security which adheres to the standards and guidelines that are known to be secure [16].

One of the key reasons for redundancy in PMU systems in smart grid is to support the requirements to be able to make security patches to the software without lost data.

We discuss the high level security requirements in general and the major security requirements and vulnerabilities in privacy, availability, integrity, authentication, authorization, auditability, nonrepudiability, third-party protection, and trust components for smart grid communications.

Smart grid is a conglomeration of different legacy systems paired with new technologies and architectural approaches, based on different standards and regulations that all need to be amalgamated into a communication network to support the challenges of the future electricity network.

The cyber security architecture for smart grid communications are being presented on the basis of cyber security and architecture requirements, dependency on legacy installations, and the regulations and industry standards.

The interconnected smart grid communication systems are riddled with vulnerabilities that vary across the networks due to the lack of built-in security in many applications and devices.

The components, systems, networks, and architecture are all important to the security design and reliability of the smart grid communication solutions.

Security services will help network operators to identify, control and manage security risks in smart grid communications.

We focus on the technologies being deployed, the key smart grid communication applications being implemented and the outlines of power industry trials that have recently been announced in privacy, integrity, and authentication and trusted computing.

Authentication and integrity can help smart grid system to protect against the most common cyber-attacks, including man-in-the-middle, forgery, impersonation, and message modification.

Since confidentiality does not merit as much concern as authentication and integrity for real-time control in smart grid, an approach that does not require an encryption step might be more appropriate.

A smart grid communication security solution requires a holistic approach including traditional schemes such as PKI technology, trusted computing elements, authentication mechanisms based on industry standards

……………(‘”,”)…….Thanks you Mam………(<,>)…….

…………………….. End……………………….