**Internet of Things in Cyber Security**

**Deepthi Thalagundamatada**

**CSC-534 Information Security Management**

**University of North Carolina Wilmington**

**ABSTRACT**

***Internet of things has been in the limelight from few years. The increase in number of Devices which are using IOT has seen rapid growth from past decade. The sophistication came along with the threats which can exploit the system by attacks. IOT has seen some attacks along with the exposure of data and uncertainty.***

**INTRODUCTION**

[1]Almost Everyone is connected to the internet today, There is increment in number of connected devices each day where it would be more than 50 billion by 2020,The Internet Of Things Signifies the transformations in the digital world that would effect each and everyone and businesses. IoT can be defined as the Physical Devices which are connected to the internet through the embedded systems, upon interaction with devices the results are generated which would be useful for the end user.

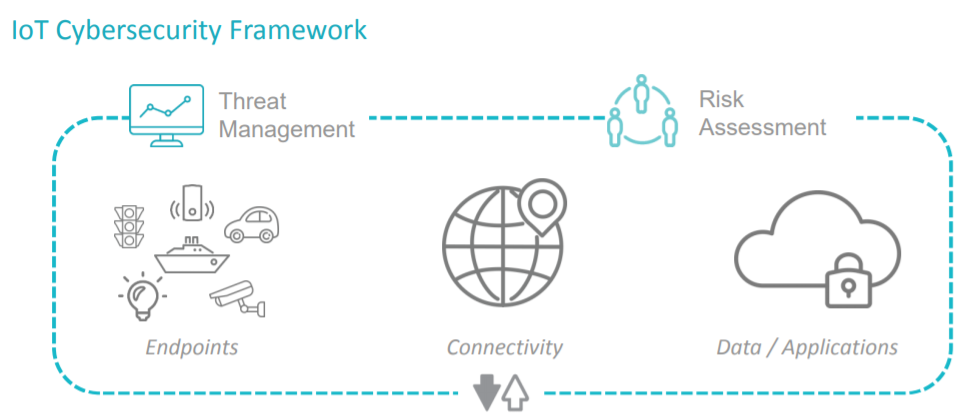
[2]IoT History can be dated back to early 1980’s when researchers at Carnegie Mellon University created a vending machine connected to the Internet. The machine delivered the information upon request. The vending machines collected the information of the stocks and refills. of stored beverage.

[3]M2M communications over the last decade provided communication paradigm along with the ability to communicate between devices autonomously without human intervention. M2M communication enabled the Practical implementation of IoT.

IoT has empowered an environment to the world which enables flexibility to provide services of all sorts, from smart environmental monitoring to smart city services to home automation to smart retail/logistics. IoT will have sensing ,visualization tools and sensing in very short time which would be accessible by everyone, from anywhere and all the time in all levels [personal, community or national level]. [2]IoT has the capability to connect the people which enables any aspect of their life towards simple change which is the making machines know what they want and ease their task and daily routine which is done through humans communicating to machines directly and indirectly, Over this the questions raise about the security problem with the possibility of impersonation, identity theft, hacking. Now a days Everything is moving to cloud and IoT is also enabled using cloud on smart devices on which has thousands of applications on it. The major another challenge would be integrating these application to work around to talk to themselves which can be coated as the integrated environments. The IoT Can not be single infrastructure as devices of different kind should be able to talk to each other, This leads to technicality challenges of the network as there are uneven networks also. As There are more number of device connected, the attention towards data privacy, data protection, safety, trust and governance is also increased from customers. Considering all the challenges and the factors we can see that there is need of the a wide-ranging strategic approach to cybersecurity. I would like to High Light the paper on proactive position to anticipate and mitigate the cyber threat.

**DISCUSSION**

There is no single solution that will secure the IoT at every level and every touch point. The only sustainable approach involves a multi-layer, end-to-end framework that takes into account all connected devices, along with the applications they run and the networks they use to transmit [5]



Just about any piece of technology that connects to a network (or cloud), provides and receives data falls under the IoT umbrella. However, the Internet of Things should realistically be broken down into three different smaller categories as not all devices are the same. After all, a router is far different from an Internet connected toaster oven. The three categories are: information technology, operational technology and smart objects ([Cisco, 2015](https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf)).

### *Review of recent attacks*

In order to better appreciate the dangers posed by cyber-attacks on critical infrastructure, we are going to review some of the most high-profile examples of cyber-attacks around the world.

#### 4.1.1. Tram Hack Lodz, Poland

In 2008 a tram system hack in the [city](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/urban-areas) of Lodz, Poland escalated to the point where a dozen passengers were injured, making this the first cyber-kinetic attack to result in [human injury](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/human-injury).

#### 4.1.2. Texas Power Company hack

In 2009 an employee that had just been fired from the Texas Power Company hacked their network to cripple power forecasting systems. He used his logins that were yet to be disabled.

#### 4.1.3. Stuxnet attack on Iranian nuclear power facility

In 2009, a worm allegedly created by U.S. and Israeli governments targeting Iranian uranium enrichment devices is believed to be responsible for causing [substantial damage](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/substantial-damage) to Iran's nuclear program by destroying uranium enrichment [centrifuges](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/centrifuge) at an Iranian nuclear facility. [Stuxnet](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/stuxnet) is a malicious [computer worm](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/computer-worms)that targets SCADA systems by targeting [programmable logic controllers](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/programmable-logic-controller) (PLCs), which allow the automation of electromechanical processes [[5]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0020).

#### 4.1.4. Houston, Texas, Water Distribution System attack

In November 2011, the [Water Distribution](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/water-supply) System at the Water and [Sewer](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/sewers" \o "Learn more about Sewers from ScienceDirect's AI-generated Topic Pages)Department for the City of South Houston, Texas was hacked.

#### 4.1.5. Bowman Avenue Dam Cyberattack

In 2013, the Bowman Avenue Dam in New York was breached and the hackers managed to [gain control](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/gain-control) of the [floodgates](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/floodgate). Investigations showed they could easily have changed the settings related to water flow or even changed the amount of chemicals used in [water treatment](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/water-treatment) to catastrophic effect. This would have led to devastating consequences.

#### 4.1.6. Ukraine power grid hacking

In December 2015, hackers managed to seize control of Ukraine's power grid's connected control system by successfully hacking the grid's [supervisory control](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/supervisory-control" \o "Learn more about Supervisory Control from ScienceDirect's AI-generated Topic Pages)and data acquisition (SCADA) system using the BlackEnergy [malware](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/malware). This caused a massive blackout that left over 700,000 people without electricity for several hours [[6]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0021).

#### 4.1.7. Dyn DDoS attack

In October 2016, Dyn–an [internet service](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/internet-services) provider, suffered a cyber-attack that disrupted access to popular websites and shut down massive portions of the internet in the United States. The hackers executed a distributed [denial of service](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/denial-of-service)attack (DDoS). The DDoS attack exploited a system known as the Mirai [botnet](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/botnets), which scans the web for poorly secured IoT devices that still have factory [default usernames and passwords](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/default-password). They then commandeered a large number of insecure IoT devices to request for services from Dyn servers. This fake traffic overwhelmed it causing the site to break. This attack succeeded largely because an astonishingly large number of people don't change default logins on their devices. Since Dyn is one of the entities that route web traffic, its going down caused a large number of websites to be unavailable for a day. Popular websites such as [Twitter](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/twitter), Netflix, Spotify, Reddit and SoundCloud were among those that were affected.

#### 4.1.8. Ransomware attack on San Francisco light rail system

In November 2016 the light-rail system of the [San Francisco](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/san-francisco) city in the US was the subject of a ransomware attack in yet another cyber incident. Quite recently, a company that makes digital teddy bears had its online database hacked and millions of [private messages](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/private-message) between parents and their children exposed. Most of these devices collect [personal information](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/personal-information) like users’ names and [telephone numbers](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/telephone-number), while others such as smart meters can monitor user activities (e.g., when users are in their houses). All these events show how easily hackers can use household or office IoT devices to spy on unsuspecting users.

#### 4.1.9. Kemuri Water Company Hack, US

In 2016, hackers infiltrated the Kemuri Water Company's water utility's control system and changed the levels of chemicals being used to treat tap water by manipulating the valves controlling the flow of chemicals.

#### 4.1.10. Smart building attack in Lappeenranta, Finland

In 2016, a targeted DDoS attack shut down heat and [hot water](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/hot-water) in two [apartment buildings](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/apartment-building) in Finland in the middle of Finnish winter.

#### 4.1.11. UK electric grid cyberattack

In July 2017, an electricity grid that supplies electricity in UK and Ireland was attacked. The cyber-attack was targeted at infiltrating the [power control systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/power-control-system), in order to enable them to take offline all or part of the electricity grid. It was carried out using some fake emails targeting some senior employees at the power company. The emails contained technical information about the grid network intended to pass them off as genuine mail but were actually intended to illicit information or make the users click on links to trigger malicious software in what is known as a [spear phishing attack](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/spear-phishing-attack).

#### 4.1.13. DDoS attack on Sweden transport network

In October 2017, DDoS attacks against the [transport network](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/transport-network) in Sweden caused train delays and disrupted travel services.

Over the years, hackers have become more capable, while most of the world's critical infrastructure systems still implement [legacy technology](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/legacy-technology), which leaves it vulnerable to even the most basic forms of cyber-attack. The increasingly interconnected nature of the infrastructure and the recent trend of rising cases of ransomware attacks across the globe is a serious cause for concern. In recent years, there have been numerous forms of malware that have been identified as targeting SCADA systems. These include Stuxnet, Havex, BlackEnergy3 and Industroyer. The fact that these malwares are specifically designed to [target infrastructure](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/target-infrastructure) means that power stations, gas plants, water plants and [transportation systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/transportation-system) are all [potential targets](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/potential-target). Since there are currently more than 6.4 billion IoT devices in use with the [number expected](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/expected-number) to rise to 50 billion by 2020, then the situation can only get worse. We are certainly likely to see more of these infrastructure targeting attacks in future.

The IoTs’ glaring insecurities were catastrophic enough when they applied to [security cameras](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/security-camera) and connected [cars](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/motor-vehicles) but they are now increasingly targeting critical infrastructure services like the smart grid. If a cyber-attack were to take down an [electrical grid](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/electrical-grids) in the dead of winter, or shut down the power to a hospital, or exploit features in smart cars while they are in motion, causing accidents on the road or even alter the temperatures in nuclear cooling towers, then the results would be catastrophic. Critical national infrastructure faces increased cases of hacking with the purpose of espionage from hostile nation-states. A cyber-attack on the infrastructure of another nation, with the aim of commandeering or disabling it potentially foreshadows the future of warfare. [Cyber security](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/cyber-security) is therefore critical to the [defense](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/defense) of a country. It also has huge ramifications to the broader economy of a country with losses from cyber theft, espionage, [disruption](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/disruptions), and [cyber terrorism](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/cyber-terrorism) currently said to be in the trillions.

Breach after breach has brought attention to the terrifying vulnerability of IoT networks and unless urgent correction measures are taken, a disaster seems inevitable in the near future as it is a matter of when not if the next attack will occur. Despite efforts to raise the cyber defense network, recent trends indicate that [human beings](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/human-species) are the weakest link in the cyber security defense network. Cases of attacks that are targeted at individuals who have access to the [critical controls](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/critical-control) of infrastructure have been on the rise. [Spear phishing](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/spear-phishing), an extremely simple attack where infected email attachments are used to illicit information or make the user click on a link to trigger malicious software have recently been used to devastating effect. This is despite the fact that spear phishing is regarded as one of the least complex forms of cyber-attack methods. This shows of low levels of cyber security awareness, even in environments that have been identified as potentially at the highest risk of cyber-attacks.

Therefore, individuals, businesses and governments must commit more resources towards becoming more cyber-vigilant, by allocating greater resources towards predicting and guarding against attacks.

### 4.2. Classification of attacks

Cyberattacks can destroy a utility's physical systems, render them inoperable, hand over control of those systems to an outside entity or jeopardize the [privacy](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/right-to-privacy) of employees and customer data. According to [[7]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0022) most attacks usually take one or a combination of four main types of attacks: device attack, data attack, privacy attack, and [network availability](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/network-availability) attack.

#### 4.2.1. Device attack

A device attack aims to compromise and control a grid [network device](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/network-device). It is often the initial step of a major attack where one compromised device is used as an entry point, to launch further attacks and compromise the rest of the smart grid network. For example, a compromised sensor might be used to send a virus disguised as genuine [sensing data](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/sensing-data) hence spreading it to the rest of the network and infecting the whole grid network. As a [cyber-physical system](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/cyber-physical-systems), the IoT-based SG with its millions of devices is at great risk since if one device in the network is compromised, the whole network becomes vulnerable. This is especially the case in Trojan horse attacks on the network. Also, due to the [high number](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/highest-number) of devices in an IoT based smart grid, auditing of the network devices to detect of any compromised device is both time consuming and untenable. Strict [access control and authentication](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/access-authentication) measures need to be effected to guard against device attacks.

#### 4.2.2. Data attack

A data attack attempts to illegally insert, alter, or delete data or control commands in the communication [network traffic](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/network-traffic) so as to mislead the smart grid to make wrong decisions/actions. Since an IoT based SG is founded on the premise of bidirectional exchange of data between the network devices and the utility, any compromise on the [data integrity](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/data-integrity) jeopardizes the justification of an IoT based SG. A commonly [observed data](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/observed-data) attack is when a customer manipulates the smart meter in order to alter his/her consumption data to reflect lower amounts in his/her [electricity bill](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/electricity-bill). Sufficient [intrusion detection](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/intrusion-detection) mechanisms must therefore be employed to ensure that the [authenticity](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/authenticity) and integrity of smart grid data is protected [8].

#### 4.2.3. Privacy attack

A privacy attack aims to learn about a users’ private or personal information by analyzing information from their smart grid [network resources](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/network-resource). Such information might include [electricity consumption](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/electricity-consumption) data where low or no usage of electricity during certain time periods might be used to infer that the location is most probably not occupied. Using such information, the perpetrator might plan [physical attacks](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/physical-attack) like [burglary](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/burglary) as no one is around. Personal information like credit [card information](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/card-information) shared with the utility provider might also be targeted in a privacy attack. An IoT based smart grid contains millions of linked user accounts which might be at risk in a privacy attack. In this era of [identity theft](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/identity-theft), users’ privacy and confidentiality must be guaranteed. Personal information must therefore be protected from [unauthorized access](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/unauthorized-access).

#### 4.2.4. Network attack

A network availability attack mainly takes place in the form of denial of service (DoS). Its intention is to use up or overwhelm the communication and [computational resources](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/computational-resource) of the smart grid network, resulting in failure or delay of communications. An example of a network availability attack is when an attacker floods a smart grid processing center with [false information](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/false-information) that it spends so much time verifying the authenticity of the information at the expense of legitimate network traffic. The center is therefore overwhelmed and not able to timely respond to legitimate thereby causing delay or failure in communications or outright [network outage](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/network-outage). Network communication in the smart grid is time critical, as a delay of a few seconds has the potential to impact on the control of grid elements resulting in irreversible damage to both the economy and security of a region. A network availability attack must therefore be handled effectively. A network attack on an IoT based SG might render millions of devices to be offline rendering the SG inoperable as the devices would be inaccessible.

All these attacks are carried out using various mechanisms [9]. The most common types of attacks are:

Malware injection, which is the installation of harmful software (viruses, spyware, rootkits, adware, malvertising, ransomware, [trojans](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/trojans) or worms) into cyberspace intended to cause damage or to disable computers and networks. A malware example is the WannaCry ransomware that has previously been used to deny people's access to essential services unless a ransom has been paid.

•

Phishing, which is a request for data from what looks like a trusted source. The aim is to trick users into believing he is trustworthy, in order for the user to do a certain action such as providing sensitive information, or clicking on a [malicious link](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/malicious-link). The most common phishing attacks are spear phishing and smishing (phishing done over SMS/text messages).

•

Hacking, which involves figuring out the password of a system's platform so as to gain access into the system. Hacking may take several forms such as brute forced attack on a system, man-in-the-middle attack or even social engineering.

•

Denial of Service, which involves flooding a system's network with high volumes of traffic and spam data. The objective is to overload it and make it slow or unresponsive due to the high number of requests [[18]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0018).

•

SQL injections are injection attacks used to attack data-driven applications where an attacker executes malicious SQL query statements targeted at a web application's database server and inserted via an input field on the client facing side of the application. Its aim is to steal, alter or delete the database contents.

•

Man-in-the-Middle Attack (MITM) attack attempts to hijack communications between the communicating devices by eavesdropping. Users at the [endpoints](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/endpoint" \o "Learn more about Endpoint from ScienceDirect's AI-generated Topic Pages)think they are talking directly to each other using their connection but in this case the adversary can view their communication and even modify it. This is especially worse in situations where the information is not encrypted.

•

An Advanced Persistent Threat (APT) is a stealthy cyberattack in which a person or group gains unauthorized access to a network and remains undetected for an extended period [[28]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0028). The goal of advanced persistent threats is most often data theft. APT involves advanced or complex processes requiring a high degree of covertness over a long period of time against specific [targeted organizations](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/targeted-organization) and are usually sponsored by nations or very large organizations. Examples of APTs include Stuxnet, which took down Iran's nuclear program, Duqu, Red October, Dragonfly 2.0 and Black Energy. [Advanced persistent threats](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/advanced-persistent-threat) typically have several phases, which can be categorized as; [Initial compromise](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/initial-compromise), Establish Foothold, Escalate Privileges, Internal [Reconnaissance](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/reconnaissance), Move Laterally, Maintain Presence, Complete Mission [[29]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0029).

Stages of APT Attacks

Initial Compromise – This stage represents the methods that attackers use to penetrate a target organization's network by exploiting vulnerable Internet-facing web servers [[29]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0029). Since an IoT SG is tightly coupled with the internet, network devices are constantly being probed by attacker for vulnerabilities.

Establishing a Foothold – Once attackers have compromised an IoT network device, they will try to access and control more devices within the victim environment. Backdoors will be installed which are used to establish an outbound connection from the victim's network to a computer controlled by the attackers.

Escalating Privileges – This involves acquiring credential items that will allow attackers to access more resources within the victim IoT environment. During this stage, attackers will try to gain access to privileged and administrator accounts. Password harvesting and cracking are some of the methods used escalate privileges.

Internal Reconnaissance – This is the stage when attacks will collect information about the compromised devices in order to obtain information about the [internal network](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/internal-network), users, groups, trust relationships, files and documents. Attackers may perform directory or network share listings, or search for data by [file extension](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/file-extension), key word, or last modified date. File servers, email servers, and domain controllers are customarily the targets of internal reconnaissance [[29]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0029), [[30]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0030).

Moving Laterally – Attackers move laterally within the IoT network to compromise more devices in order to search for specific data.

Maintaining Presence – Attackers install backdoors to continue control over the IoT devices remotely from outside network. Different backdoors from the ones used during the Establish Foothold stage make them difficult to identify and remove all of their access points. Attackers could also cover their tracks by eliminating traces of compromised devices by deleting activity logs and encrypting their communication traffic [[29]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0029), [[31]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0031).

Completing Mission – Once the attackers are successful in finding files of interest on compromised IoT devices, they pack them into archive files and transfer out using FTP, custom file transfer tools or backdoors.

It is predicted that IoT [security breaches](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/security-breach) will continue to increase as the number of IoT devices multiply coupled with the rise in number of mobile devices and penetration of internet services. As a result, more and more internet-connected devices could be a target for [cyber criminals](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/cyber-criminal) trying to hold users’ [personal data](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/personal-data) at ransom. Hence, smart systems will be tested to their limit.

### 4.3. Mitigation of attacks

New threats are emerging everyday some of which have previously been unknown making it very hard to eliminate cyber security attacks. This makes cyber-attacks [mitigation plans](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/mitigation-plan) to be of [utmost importance](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/utmost-importance) as they provide the first line of defense in case of future attacks. Mitigation of attacks involves both [attack prevention](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/attack-prevention) methods and attack detection methods. Some of the mitigation plans are outlined below.

#### 4.3.1. Access controls

These are rules which are defined in advance to define which resources, data files or devices a user or a device is to be [granted access](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/granted-access) to and which he/it should have no access at all. Using these predefined [access privileges](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/access-privilege) to grid devices and system [functionalities](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/functionality) reduces likelihood of malicious access to network devices. Access controls such as [Discretionary Access Control](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/discretionary-access-control) (DAC), [Mandatory Access Control](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/mandatory-access-control) (MAC) and Role Based Access Controls (RBAC) can increase the system reliability and eliminate potential [security threats](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/security-threat) [[32]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0032). Since IoT based SG is a cyber-physical system that is monitored and configured [remotely, access](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/remotely-access) controls are vital in order to limit users’ and devices access in the network.

#### 4.3.2. Encryption

When deploying IoT solutions, there is need to encrypt traffic flowing between IoT devices and the control centers including the utility provider's servers. Ensuring that the communications are encrypted using strong [encryption](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/cryptography) tools is crucial as it reduces an attacker's ability to either hijack communications or generate valid data in order to fool the system. This ensures that both the integrity and confidentiality of [data communications](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/data-communication) is maintained.

#### 4.3.3. Authentication

This involves identifying devices in the network and authorizing what each device should carry out in the network. [Device authentication](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/authentication-device) is normally the first step of a data communication session, and its result is often a shared session key for encrypting and authenticating subsequent [data packets](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/data-packet) and ensuring data integrity. Due to the [time-sensitive](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/time-sensitive) and traffic-intensive nature of IoT smart grid communication, an authentication scheme should involve minimal exchange of messages between the grid devices. Authentication ensures meter will not accept commands from an unauthorized 3rd party [[33]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0033). Authentication involves both identification and [authorization](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/authorisation).

#### 4.3.4. Regular security patches and updates

IoT devices should be easily upgradable so that bugs and [security updates](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/security-update) can be deployed in an easy and manageable way. Unfortunately, most manufactures currently build devices without thinking about deploying future [firmware updates](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/firmware-update)at all. However, they need to appreciate that due to evolution of technology, [operating systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/computer-software) and [application code](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/application-code) may be faced by [emerging threats](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/emerging-threat) and vulnerabilities in future and that the rollout of updates to address these issues is paramount. Deploying firmware updates can be tricky if they're not configured to receive the updates. Considering the sheer size of an IoT smart grid, regular update to upgrade the firmware is the logical and reasonable solution as compared to a large-scale replacement of the obsolete devices. Cyber security challenges are particularly amplified when businesses integrate new and old systems without regard to overall [network security](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/network-security). Hence, ensuring a consistent process that allows for flexible firmware deployment will allow the patching up of security loopholes across the network hence mitigating [potential threats](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/potential-threat) [[34]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0034).

#### 4.3.5. Physical security

The [physical security](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/physical-security) of connected grid devices is of utmost importance. Tamper-proof mechanisms should be employed and integrated into grid components to safeguard them from physical unauthorized access. The [physical access](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/physical-access) by [unauthorized personnel](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/unauthorized-personnel) might result in data stored in the devices being compromised. Such data might include authentication, identification, usage and [account information](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/account-information). [Remote wiping](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/remote-wiping) capabilities should therefore be in place to erase or lock network devices to protect sensitive private data from leaking as they might be used maliciously by the intruders. Also equally important is the physical security of the premises where the servers and the [control rooms](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/control-room) are located. These provide a [central location](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/central-location) from where [easy access](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/easy-access) to the whole IoT smart grid is easily available for anyone intending ill harm to the grid such as hackers and from disgruntled former or current employees. They therefore have to be secured as they pose a risk to the security of the whole network [[35]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0035).

#### 4.3.6. Backdoors and logins

When developing IoT SG solutions it is vital that the integrity and security of the [end user](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/end-users) is maintained. Although argument has been made for provision of a backdoor in these devices that can be used for surveillance and [law enforcement](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/law-enforcement)purposes, it is important to note that this is a double-edged sword and the same backdoors are the ones that are later utilized by [criminal elements](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/criminal-element) trying to gain illegal access to the devices. Manufacturers must therefore ensure that no backdoor or [malicious code](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/malicious-code) is deployed on the devices. They should also ensure that they do not mass produce devices with a single set of default logins but rather should create unique logins for each and every device. This will make the devices harder to compromise or even commandeer as botnets to participate in DDoS attacks.

#### 4.3.7. Intrusion Detection Systems (IDS)

All the above-mentioned cybersecurity mitigation techniques are applicable when defending the IoT smart grid against attacks initiated by an antagonist outside the grid. However, if the antagonist is already inside the system, then these mitigation techniques will be ineffective. Intrusion detection mechanisms are therefore important in order to identify and isolate compromised networks and/or devices. This will help trigger [early warning systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/early-warning-system) in order to effect [counter measures](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/countermeasure) to take appropriate actions in advance to mitigate any forthcoming attacks or to roll back any harmful changes done on the system [[23]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0023), [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0036). This can be effected using firewalls and antivirus. The main intrusion detection techniques are:

(a)

Signature Based IDS

The Signature Based Detection compares a possible threat with the attack type already stored in the IDS database. The limitation of this type of detection technique is that only those intrusions whose signature is available in the database can be detected and if any new type of threat comes which is not already known to the IDS, the system becomes vulnerable to that attack [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0036).

(b)

Anomaly Based IDS

The anomaly-based IDS is a dynamic behavior-based detection technique by which the IDS looks for vulnerabilities based on rules set forth by the user and not on the basis of signatures already stored in the IDS. This type of detection applies [Artificial Intelligence](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/artificial-intelligence) to distinguish between normal traffic and anomalous traffic hence is able to detect unknown or new attacks. However, since not all abnormal traffic is malicious, this technique results in more false positives and is therefore more effective when used to [generate alerts](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/generate-alert) and a human agent evaluates each flagged event for the appropriate action to take [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0036).

(c)

Host Based IDS

Host [Intrusion Detection System](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/intrusion-detection-system) (HIDS) is installed on a host in the network. It collects and analyzes the traffic that is originated or is intended to that host. HIDS leverages their [privileged access](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/privileged-access) to monitor [specific components](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/specific-component) of a host that are not readily accessible to other systems. This intrusion detection scheme can only detect [malicious activities](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/malicious-activity) for a particular host on which it is installed and have a limited view of entire network [topology](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/topology) [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0036).

(d)

Network Based IDS

Network IDS (NIDS) works by monitoring the traffic as it flows through the [network infrastructure](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/network-infrastructure). Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network. NIDS should be capable of analyzing a large amount of network traffic in a timely manner in order to remain effective [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0036), [[37]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0037).

(e)

Stack Based IDS

Stack based IDS works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers. Watching the packet in this way allows the IDS to pull the packet from the stack before the OS or application has a chance to process the packets [[36]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0036).

#### 4.3.8. IP fast hopping

Since Denial-of-Service attacks are the largest threat to the IoT an effective [network layer](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/layer-network) [software solution](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/software-solution) is needed to mitigate against DDoS attacks. IP fast hopping provides an easy way for clients to hide content and [destination server](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/destination-server) of their communication sessions. It does this by hiding the real IP address of a server behind a large pool of IP addresses belonging to a number of routers in different networks hence prevents identification of destination of network traffic [[38]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0038). The real-time changing of server's IP address is done simultaneously at both the authorized clients and the server and is according to a unique schedule which is only available to both.

### 4.4. Security standards for the Smart Grid

Resilient [information and communications technologies](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/information-technology) are a prerequisite for [reliable operation](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/reliable-operation) of smart grid.

Because an IoT smart grid is highly dependent on [ICT](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/information-technology) and interconnected with the Internet, there is a strong need for the assurance that information technologies embedded in the smart grid will not induce failures or facilitate the intrusion by [malicious agents](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/malicious-agent). Unfortunately, many of these systems were designed and built at a time when defending against malicious attackers was not a priority, because such attacks were rare and systems were much less interconnected than they are today. Furthermore, because of the typically long lifetime of [automation systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/automation-system)of up to several decades, improvements can only be made gradually and over time. Nevertheless, in recent years efforts have been made to address these issues by creating new standards that describe how to augment decades-old systems and protocols so that they can offer better protection against [malicious attacks](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/malicious-attack). Many different standards have been proposed for international standardization of activities in the field of smart grid technologies. These standardized solutions and practices can be applied to provide systematic [security assessment](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/security-assessment) methodologies of smart grid components so that the reliable and [secure operation](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/secure-operation) of the grid can be guaranteed. Chief among them are the International Electrotechnical Commission (IEC) 62351 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 [[39]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0039). The [practices recommended](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/recommended-practice) in the standards, offer high level of assurance that they are systematic, complete and secure, as they were evaluated by numerous experts in a long-term process [[40]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0040), [[41]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0041). These standards address security issues in existing systems, enable their certification, [gain credibility](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/gain-credibility) of customers and building a [competitive advantage](https://www-sciencedirect-com.liblink.uncw.edu/topics/social-sciences/competitive-advantage)among other organizations in the sector [[42]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622" \l "bib0042).

i.

International Electrotechnical Commission (IEC) 62351

IEC 62351 is an [industry standard](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/industry-standard) aimed at improving security in automation systems in the power system domain. It contains provisions to ensure the integrity, authenticity and confidentiality for different protocols used in power systems. IEC 62351 in particular addresses security in systems and protocols that are predominantly used in automation systems in the electricity distribution domain. Like many of these standards, it is not a revolution, but a careful evolution, to address security issues without completely breaking [backwards-compatibility](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/backward-compatibility) and [interoperability](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/interoperability) with [legacy systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/legacy-system) [[42]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0042).

ii.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82

NIST Special Publication (SP) 800-82, provides guidance on how to secure [Industrial Control](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/industrial-control) Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, [Distributed Control Systems](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/distributed-control-system) (DCS), and other control [system configurations](https://www-sciencedirect-com.liblink.uncw.edu/topics/computer-science/system-configuration) such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and [safety requirements](https://www-sciencedirect-com.liblink.uncw.edu/topics/engineering/safety-requirement). SP 800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks [[39]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0039), [[42]](https://www-sciencedirect-com.liblink.uncw.edu/science/article/pii/S1874548217301622#bib0042).

**CONCLUSION**

**REFERENCES**

[1] <https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf>

[2]<https://www.blueboltsolutions.com/the-impact-of-internet-of-things-iot-on-cybersecurity-2.aspx>

**[3]** J. Wan, M. Chen, F. Xia, D. Li and K. Zhou, From Machine-to-machine communications towards cyber-physical systems Computer Science and Information Systems (ComSIS), vol. 10, no. 3, pp. 1105–1128, 2013. doi:[10.2298/CSIS120326018W](http://dx.doi.org.liblink.uncw.edu/10.2298/CSIS120326018W).

**[4]** B. Miller and D.C. Rowe, A survey of SCADA and critical infrastructure incidents in *Proceedings of the First Annual conference on Research in Information Technology*, Calgary, 2012. doi:[10.1145/2380790.2380805](http://dx.doi.org.liblink.uncw.edu/10.1145/2380790.2380805).

**[5]** <https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf>

[6] R.M. Lee, M.J. Assante and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid Electricity Information Sharing and Analysis Center (E - ISAC), 2016.

[7] X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, Securing smart grid: cyber attacks, countermeasures, and challenges *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.

[8] S. Mishra, X. Li, A. Kuhnle, M.T. Thai and J. Seo, Rate alteration attacks in smart grid in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*