ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY

Kanyakumari Main Road, near Anjugramam, Palkulam, Anjugramam, Tamil Nadu 629401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ADD ON COURSE

IOT AND SOCIAL MEDIA SECURITY

COURSE MATERIAL

IOT & SOCIAL MEDIA SECURITY

1 IoT Security

1 Introduction to IoT

Networks of objects, devices or items that are embedded with sensors are referred to as the Internet of Things (IoT). These devices can communicate with one another for data exchange. IoT creates various ways of direct integration between physical world and computer-based systems by remote sensing and controlling of objects across current network infrastructures. The major benefits obtained are improved efficiency, accuracy and economic related factors.

2 Applications of IoT

User can uniquely identify the object associated with the network. Experts estimate that IoT would consist of almost 50 billion objects by 2020. Security and privacy are the two major issues faced by IoT. Since IoT involves communication of devices, maintaining security among them becomes critical at some instances. Despite having many challenges, IoT has numerous applications and scope. Some of them that play an emerging role in current world can be listed as follows,

- Smart Cities
- Smart Environment
- Smart Water
- Security &Emergency
- Retails
- Logistic
- Industrial Control
- Smart Agriculture
- Smart Animal Farming
- Domestic and Home Automation
- Health care

The core application areas include Agriculture, Healthcare, Retail, Transport, Environment, Supply Chain Management and Infrastructure monitoring. Figure 1 depicts some example applications of IoT.

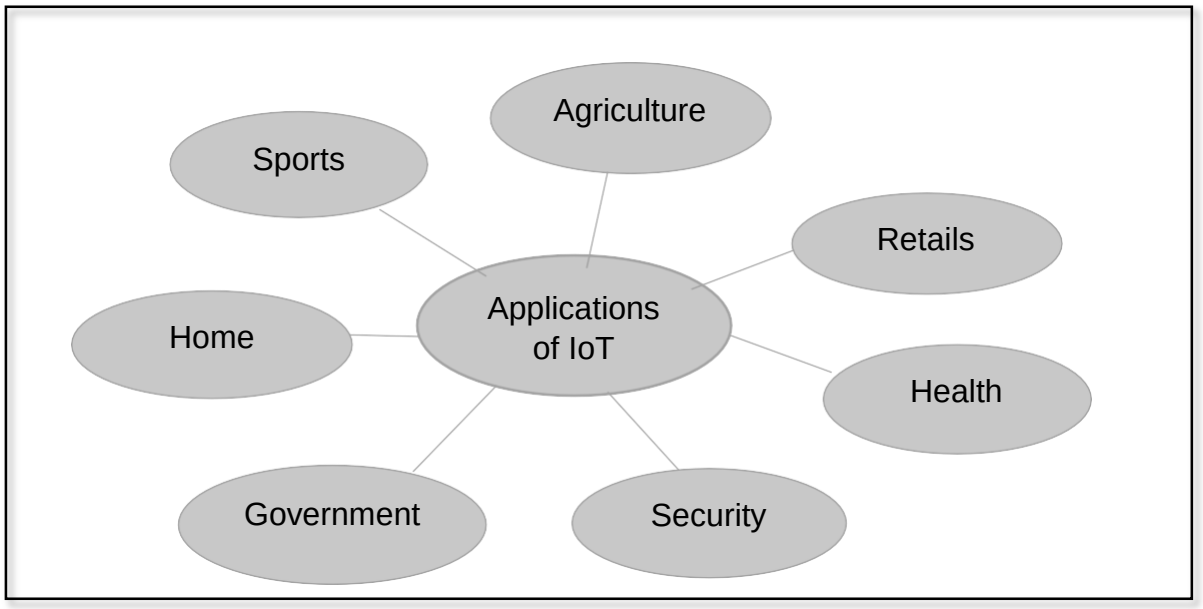

Figure 1 Applications in IoT

Apart from the above applications there are new applications emerging in the near future based on IoT. Since these applications are network based, they face issues in ensuring security.

3 Challenges in IoT

There are considerably Wide varieties of issues faced by IoT today. An overview on the major types of issues can be covered under five basic topics as follows,

i. Privacy
ii. Security
iii. Interoperability
iv. Regulatory, legal, and rights issues and
v. Other general issues.

Among the five major challenges listed above, the privacy and security challenges are considered as the most important challenges due to data compromise. Now-a-days devices handle personal data through Internet where they are exposed to various attacks. Therefore, users must be aware of these attacks when operating on unsafe environments to prevent themselves from becoming victim to attackers.

Figure 2 shows the classification of general challenges in IoT.

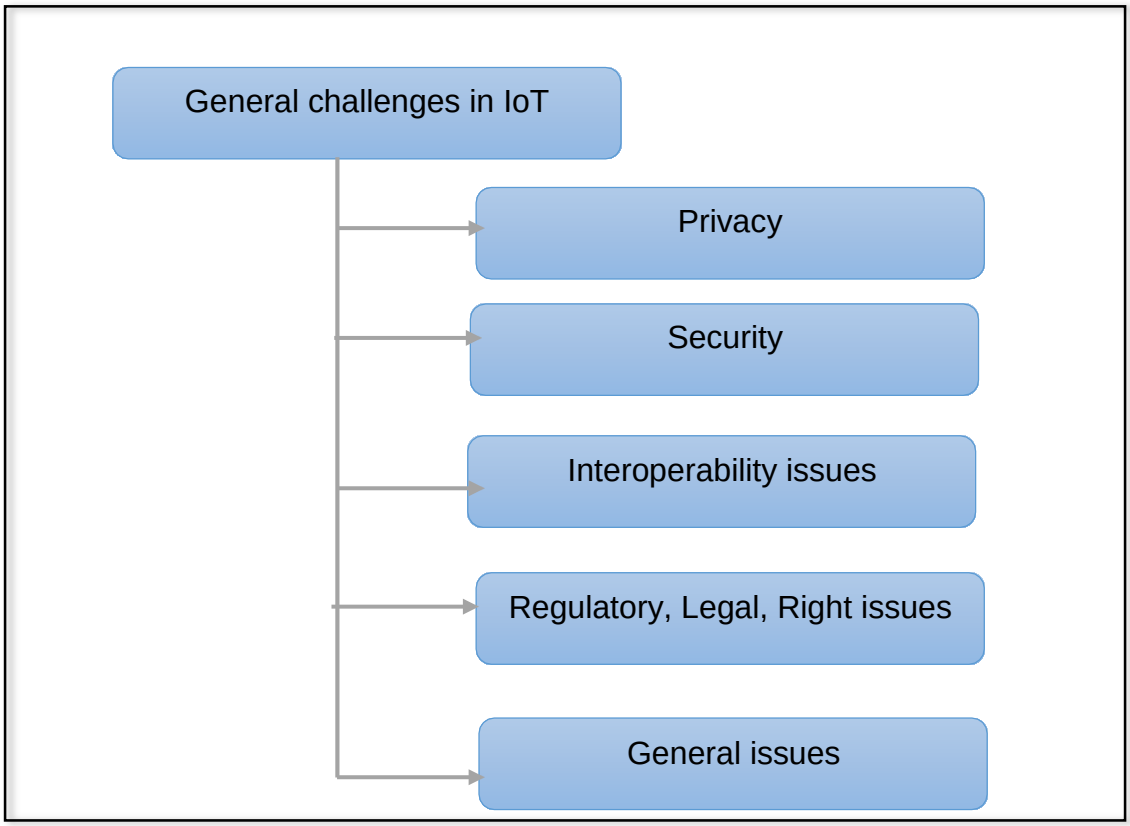

Figure 2 General challenges in IoT

1 Privacy Aspects of the Internet of Things

Privacy will become a major challenge to IoT devices when users exchange information over Internet or store data in the cloud. Privacy concerns must be taken into consideration for expanding the feasibility, reach of surveillance and testing of IoT.

2 Security Challenges due to IoT Devices

IoT devices are Internet connected devices that differs from traditional computers or devices and face the following security challenges,

- The homogeneity of the complete IoT device deployments having same characteristics results in security vulnerability like data exposure.
- Most of the IoT devices are deployed with long life-time with high technology features. They can also be installed under conditions which are difficult to upgrade, or face situations when they will be no longer available in the company that manufactured them or with less support warranty.

- The IoT devices designed with improper upgradation features makes the maintenance of security highly complex.
- The IoT devices are configured with invisible internal working and production of precise data streams. This makes the user ignorant of the internal functioning of devices paving way to security vulnerabilities. The improper actions like collection of unwanted data when connected to Internet may lead to a security breach.
- The IoT devices deployed in improper physical environment is also prone to security threats while attackers have direct physical access to those devices.

3 Challenges in IoT Interoperability / Standards

The primary issues faced during the early development and adoption of IoT devices are as follows

- **Interoperability** – It is the ability of IoT systems or software to exchange and make use of information. When this property fails, the data associated with these systems are corrupted and are prone to various issues.
- **Standards** – Some IoT devices face challenges when these standards are violated under certain conditions.
- **Protocols** – During unfavourable situations, the devices may fail to follow these essential leading to vulnerabilities.
- **Conventions** – When user is unaware of the common conventions used in IoT, leaving users to face serious trouble.

Apart from the above other challenges and considerations may include the following,

- Proprietary Ecosystems and Consumer Choice
- Technical and Cost Constraints
- Schedule Risk
- Technical Risk
- Devices Behaving Improperly

4 Regulatory, Legal, and Rights Issues

IoT applications face a wide range of challenges due to regulatory, legal and rights issues. At times, IoT devices increase the cause of legal issues due to violation of legal rights and concerns. Several regulatory and legal issues that affect the IoT applications can be listed as follows,

- Data Protection and Cross border Data Flows
- IoT Data Discrimination
- IoT Devices as aids to Law Enforcement and Public Safety
- IoT Device Liability
- Proliferation of IoT Devices used in Legal Actions

Apart from regular challenges there are certain general challenges available.

5 General Challenges in IoT Connectivity

Some general challenges in IoT connectivity are listed below.

- Signalling
- Presence detection
- Power consumption
- Bandwidth

The above section discusses the major challenges faced by IoT. Of all the challenges listed, security is the most important issue to be considered when IoT devices are connected through sensor networks. This is because the communication are not as secured as concerned.

IoT Security Definition

IoT security refers to the process of ensuring security between the network and connected devices in the Internet of Things (IoT). The devices involved in IoT interconnection are mechanical and digital devices, computing environments, people, objects and animals. These are provided with a unique identifier and have the ability for automatic data transmission across the network. Since connection of these devices and communication are through the Internet, the chances of vulnerability exploitations are more prominent. This makes the implementation of security solutions in IoT device connections slightly complex. Major security concerns while developing IoT enabled devices are

- Data Encryption
- Data Authentication
- Side-Channel attacks

1 Data Encryption

Internet of things applications contain large data set where processing and retrieval of those data play a fundamental role in the IoT domain. Majority of the data are personalized which is to be encrypted necessarily. When data is processed online it requires a Secure Socket Layer protocol or SSL certificate for security purposes. This certification is used for encrypting and protecting the online user data by the websites. In addition to this, encryption and protection of wireless protocol is also a must during data transmission across wireless networks. Only authorized users are able to know their sensitive data location. Hence, it is important to make sure that a wireless protocol with built-in encryption is used.

2 Data Authentication

The devices and application are still prone to attacks even after successful data encryption. A security compromise due to the lack of authenticity may take place during data communication between IoT devices. For example, when a temperature sensor is set for smart homes, an attacker can setup fake data or compromise sensor data which may lead to a disastrous situation. This may involve instructions to raise temperature, cool down under any environmental conditions. Hence authenticity of data and encryption are very important. Despite lack of authentication having indirect consequences, the attackers may also cause severe security issues depending on the importance of data.

3 Side-channel Attacks

Apart from encryption and authentication, there are also other attacks called side- channel attacks. These attacks target on how the information is displayed rather than the information itself. IoT applications such as timing information, power consumption or electromagnetic leak can be exploited by side channel attacks during data access on these systems.

Figure 3 shows an example of a side-channel attack.

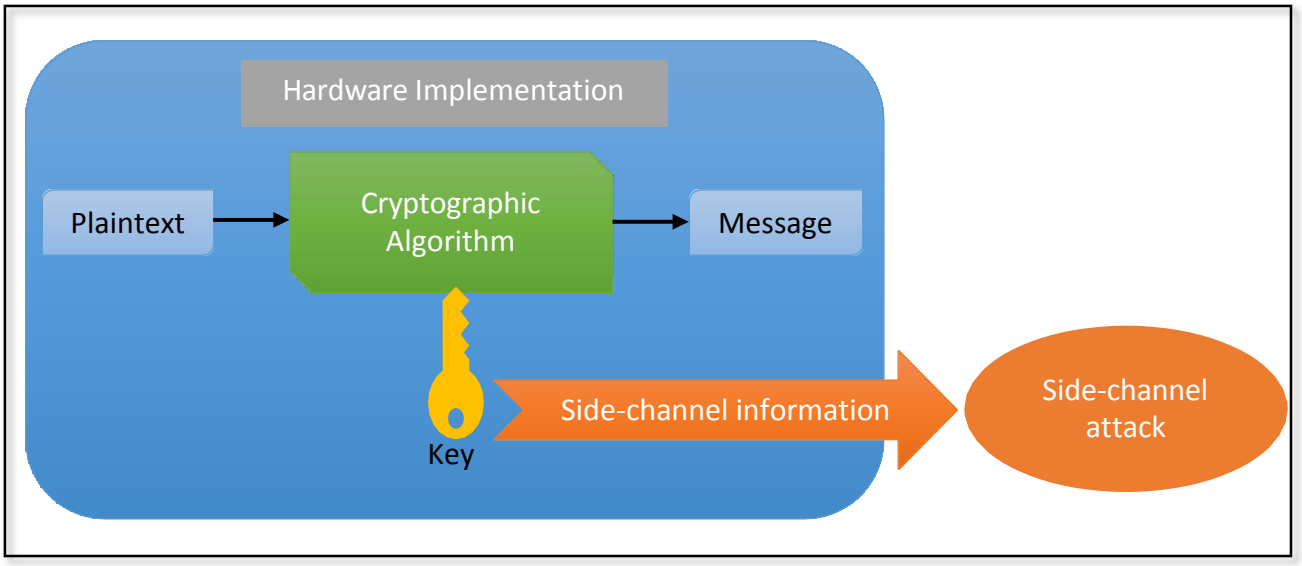

Figure 3 An example of Side-channel Attack

The role of security is not considered as important during the design phase of a product. However due to the evolution of network connected appliances and objects. This poses IoT devices to face several risks such as device security and end-to-end security compliances in the IoT environment. Some of the security challenges faced by IoT can be defined as follows,

- Using embedded or default passwords are weak password types that lead to data security breaches. They also pave way to gaining of access to IoT devices due to weak password mechanisms.
- As most of the IoT devices are not provided with advanced security features, they lack some resources that is essential in implementing system security. Some of the issues that manufacturers face during security are cost issues, system slow down and improper functioning of devices. For example, sensors that monitor humidity or temperature cannot handle advanced encryption or other security measures due to lack of resources to handle the strong security solutions.
- Another challenge occurs due to IoT connectivity that do not contain built-in legacy assets required for connection. Replacement of these infrastructures causes for- bidden costs. Hence, smart sensors should be complemented with other assets.
- System updates support features only for a particular timeframe i.e., it is preset to function for limited span of time. Therefore, the security challenges of IoT devices are

possibly high in long-time functioning. Hence, system updates need a combined support and features of legacy and new assets.

- Large organizations and industries use standards and frameworks to secure IoT devices from attacks over networks. Despite all these security standards, there is no single agreed framework. IoT security is disturbed due to the lack of industry-accepted standards, as they are proprietary and incompatible to implement. This makes security systems and interoperability difficult to manage.
- Providing secure systems and end-to-end security are major challenges faced by security teams outside the expertise realm due to the convergence of IT and operational technology (OT) networks. To prevent IoT security, implementing IT teams with necessary skill sets and usage of a learning curve should be put forth.

Attacks on Service Oriented Architecture Layers

IoT Security is considered as a very important task both at device level and its operations level especially, in the Service Oriented Architecture (SoA). Security in SoA is not a simple concept. It is defined under various layers. SoA ensures the interoperability between heterogeneous devices in multiple ways which consists of four layers with the distinguished functionalities namely,

- Sensing Layer
- Network layer
- Service layer
- Interface Layer

a) **Sensing Layer** – Sensing layer is integrated with available hardware objects to sense the position of things.

b) **Network Layer** – Network Layer is the framework to support over wireless or wired connections among the things.

c) **Service Layer** – Service Layer is to create and manage services required by users or applications.

d) **Interfaces Layer** – Interfaces Layer consists of the interaction methods with users or applications

Therefore, attacks on each layer are a possibility.

Figure 4 shows the classification of various attacks on SOA layers.

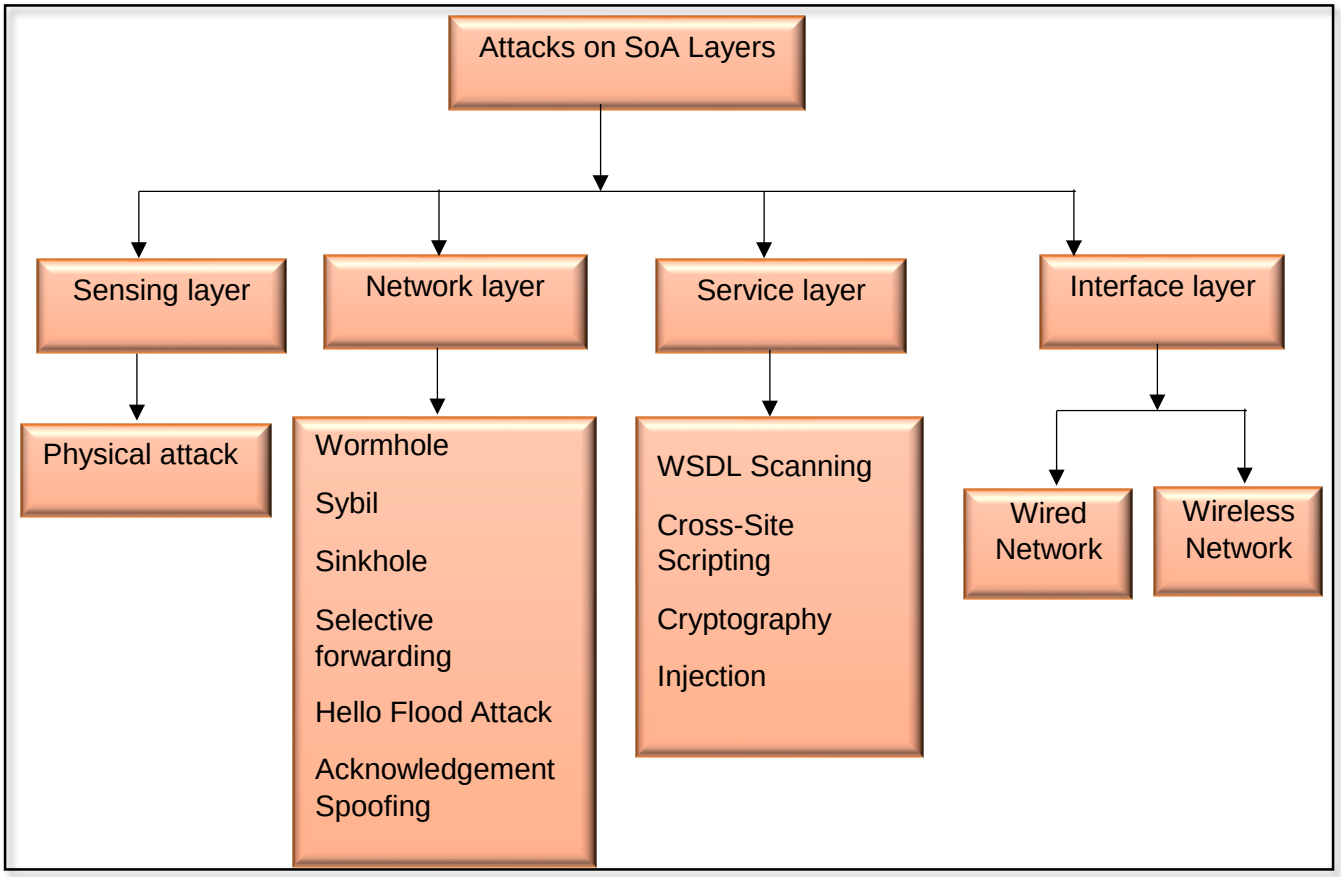

Figure 4 SOA Layer Attacks

1 Sensing Layer Attacks

The sensor layer is the most sensitive layer where attackers can easily carry out physical attacks. These may include data theft, data loss, destroying computer resources. Hence, it is necessary to protect the confidentiality and integrity of data. This can be done by preserving the confidential data such as blood pressure reading, or account details stored or collected in sensors through authorized access

2 Network Layer Attacks

This layer is helpful in transferring the information across various networks and IoT devices. During this process, there arises various network issues that can be complemented by implementing network management technologies for heterogeneous networks such as fixed, wireless, mobile, etc. In addition, network energy competence, security, and privacy procedures must also be in place. The most general types of network layer attacks are:

- Wormhole Attack

- Sybil Attack
- Sinkhole Attack
- Selective Forwarding
- Hello Flood
- Acknowledgement Spoofing

i. Wormhole Attack

In this type of attack, the attacker reports packets at a particular network node, passes them to another node, and retransmits them into the specific network. An example for wormhole attack is displayed in figure

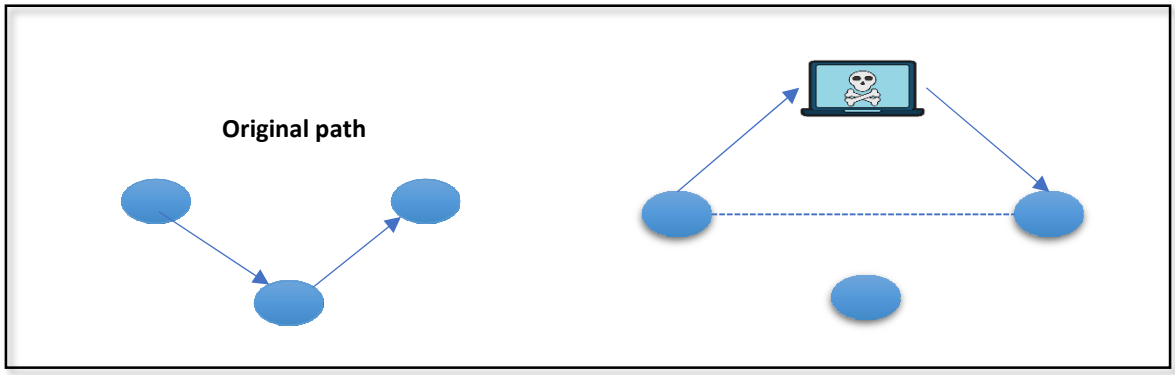

Figure 5 An example for Wormhole attack

ii. Sybil Attack

In this attack, the opponent sensor node accepts several characteristics to all other sensor nodes in the WSN reducing the efficiency of WSN. This results in occurrence of false nodes at various places at a time. By altering the security keys and resetting network devices can help in preventing this type of attack. An example for sybil attack is displayed in figure

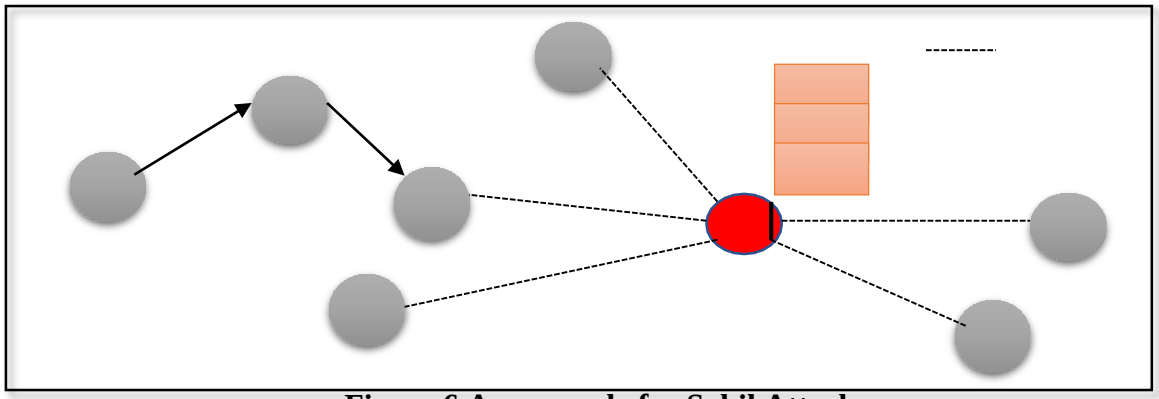

Figure 6 An example for Sybil Attack

iii. Sinkhole Attack

Here, the attacker concedes a specific node and makes it more irresistible to adjacent nodes through false routing information. In order to attract the whole network traffic, Malicious sensor nodes appear as black hole. Hence, Sinkhole attack is otherwise known as Black hole attack. An example for sinkhole attack is displayed in figure

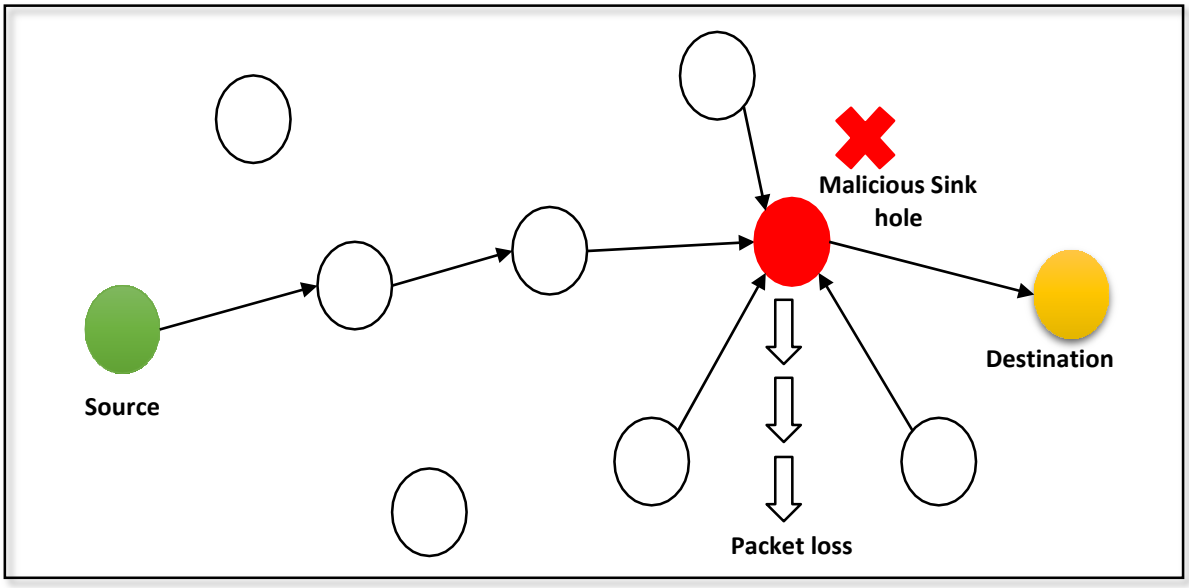

Figure 7 An example for Sinkhole attack

iv. Selective Forwarding

In this type of attack, the attacker selects and forwards only a particular sensor node data which is malicious. This differs from the ad-hoc networks, where all nodes accurately frontward the acknowledged data. An example for selective forwarding attack is displayed in figure 8.

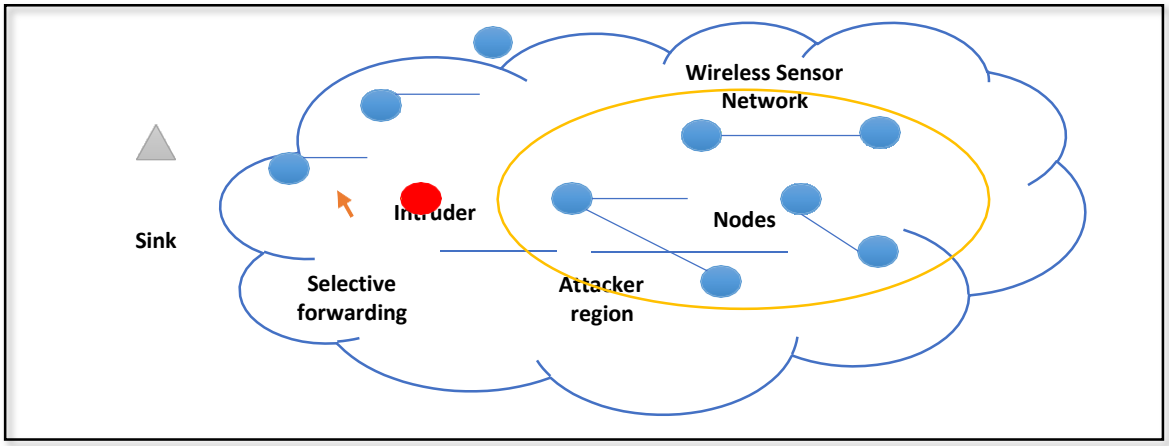

Figure 8 An example for Selective Forwarding attack

v. Hello Flood

It is essential to transmit HELLO packets to the adjacent nodes in WSN through several routing protocols. The sensor nodes that lies within the frequency of the sender node must receive these messages. Occasionally an attacker may proliferate routing or other information with suitable frequency thereby boosting the adjacent network nodes to accept the packets. An example for HELLO flood attack is displayed in figure 9.

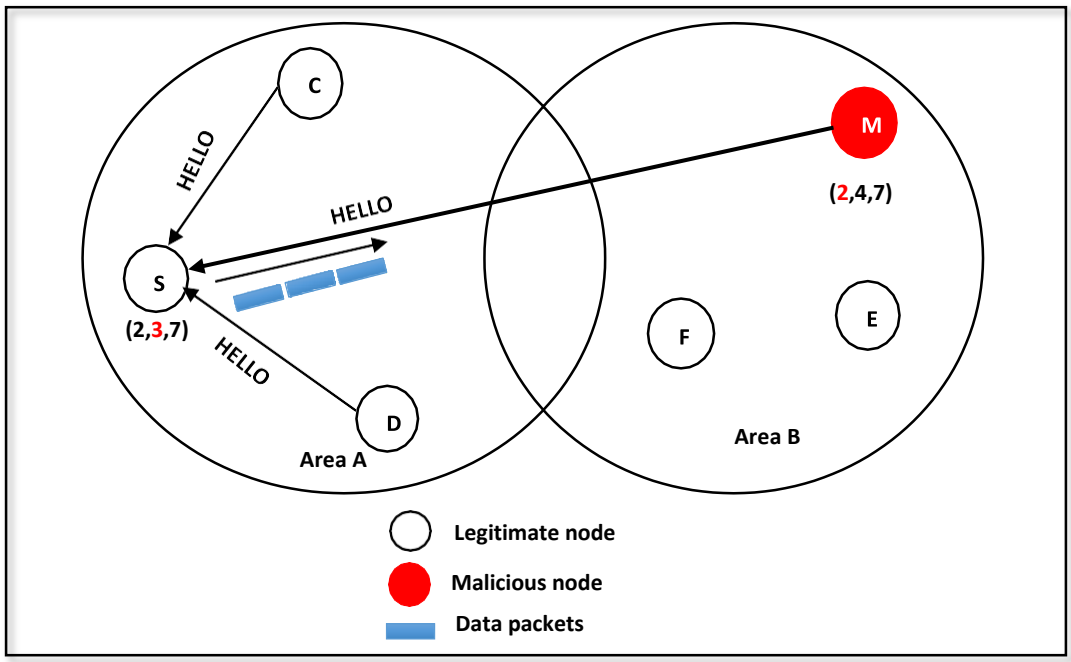

Figure 9 An example of HELLO Flood attack

vi. Acknowledgement Spoofing

The usage of routing algorithms in a network sensor node requires acknowledgements to be established. This acknowledgement of an eavesdropped packet can be spoofed by the adversary node caching false information to the neighbor nodes. An example for Acknowledgement spoofing is displayed in figure 10.

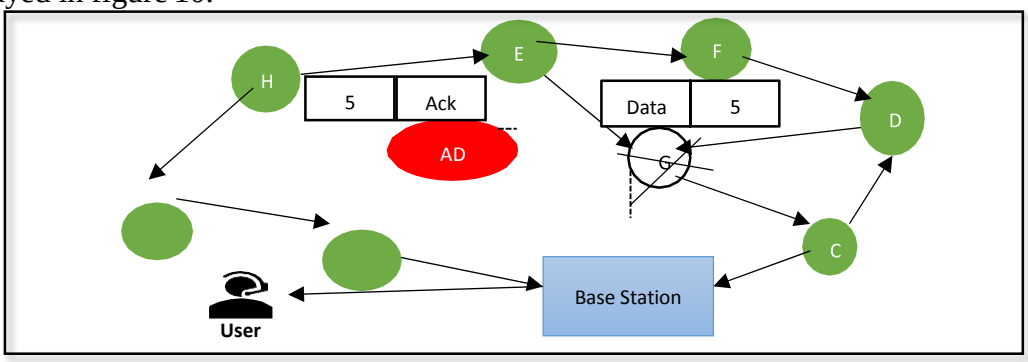

Figure 10 An example for Acknowledgement Spoofing

3 Service Layer Attacks

The vital service in an IoT application is the use of middleware technology relied upon by the Service layer. The use of this technology is that it offers a cost-effective medium, where re-usage of hardware and software platforms are done. The Service APIs are responsible in offering user service interactions. The service layer attacks are further divided into three types namely,

- Web Services Description Language scanning
- Cross-Site Scripting
- Injection

i. Web Services Description Language (WSDL) scanning

A Web service's WSDL statement presents its processes, constraints and web attachments. The service providers are only allowed to make use of the internal operations such as admin activities. The remaining peripheral processes can be instantiated by any service consumer. An attacker guesses the tag associated with the internal operation and initiate it with the help of web service endpoints available in its WSDL statement. This is known as the WSDL scanning.

ii. Cross-Site Scripting

These are types of injection attacks that takes place by the attacker injecting malicious codes into the trusted websites or application scripts. It usually occurs in the browser side script, to a diverse user end. These Flawed codes are spread across various websites and also displayed on user web application where an input is given by the user that generates outputs without authorizing or encrypting it.

iii. Injection

It is the general form of attack performed by the attackers. Here the adversary alters a back-end command statement with the help of un-sanitized user input.

4 Interface Layer Attacks

IoT includes various device types which are provided by diverse vendors. This results in the lack of standard compliances. The interface layer attacks are further classified into two types namely, wired network and wireless network as displayed in figure 1

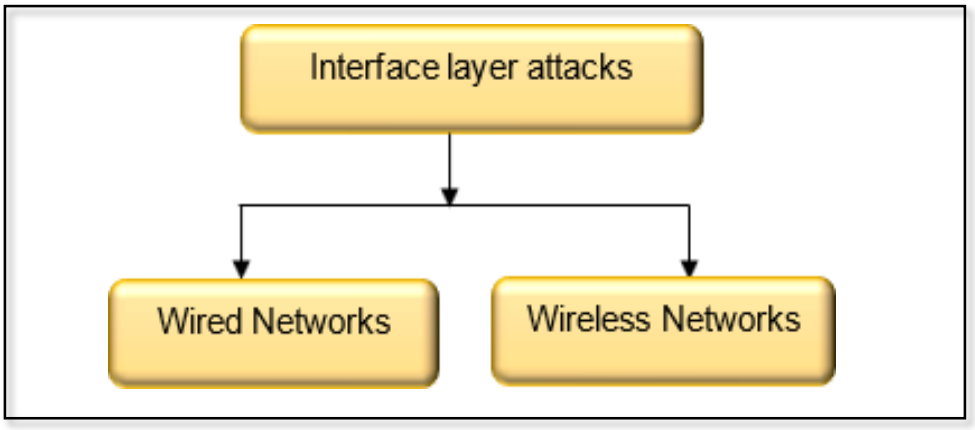

Figure 11 Attacks on Interface Layer

i. Wired Networks

This network makes use of cables to link equipments to the network or other networks. The connection takes place by connecting the ethernet ports on a network router at one end of the cable to any device type at the other end of the cable. The various types of wired network attacks are:

- Content Address Memory (CAM) table exhaustion attacks
- Address Routing Protocol (ARP) spoofing
- Dynamic Host Configuration Protocol (DHCP) starvation

a. Content Address Memory (CAM) table exhaustion attacks

The data link layer reports data packets with respect to the end point of hardware's physical Media Access Control (MAC) address. The Content Address Tables (CATs)are maintained by the network switches mapping the port switches to definite MAC addresses. A CAT Table Exhaustion Attack mostly turns a switch into a hub thereby flooding it with new MAC-to-port corresponding's until reaching the maximum table's fixed memory.

b. Address Routing Protocol (ARP) spoofing

At the data link layer, the network layer assigns a logical IP address and translates it into a physical MAC address. For ensuring reliable data communication, every network switch must contain an updated table for mapping logical address (IP) to physical(MAC) addresses. In an ARP spoofing attack, the rivalry radiates the target system's IP address in addition to its original MAC address. An example for ARP Spoofing is displayed in figure 1

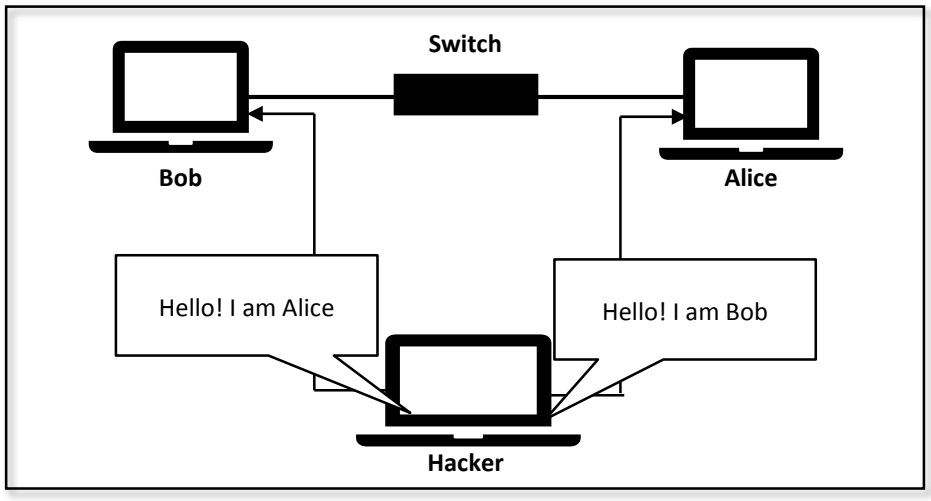

Figure 12 An example for ARP spoofing

c. Dynamic Host Configuration Protocol (DHCP) starvation

In this attack, the opponent fails to confirm the response after receiving the IP address and lease period from the DHCP server. Despite, the DHCP server is flooded with IP address requests until the server's memory is fully-filled. During this time, any host request for joining the link will be given refused access, causing Denial of Service (DoS) attack, that paves way to other subsequent attacks.

ii. Wireless Networks

The wired cables and various network equipment's are replaced by wireless networks. This type of wireless connections helps in reducing the cost at homes, large organizations and other telecommunication networks. Any type of devices such as computers, laptops, mobile phones, PDA's can be connected to a wireless network with the help of frequency available. The various attacks that takes place on wireless networks are:

- Hidden nodes
- Deauth(De-authentication)

a. Hidden nodes

Consider an example where Node A initiates the communication with Node B that waits for the broadcast. Here, the Node A is hidden and so the Node B cannot have a direct communication with A and has to wait with respect to the access point

communications. Hence, the adversary exploits this usability by overflowing system with CTS (Clear to Send) messages.

b. Deauth (De-authentication)

A new client joining a wireless network for the foremost time is authenticated by the access point (AP) and later linked to the specific access point. The client is isolated from the access point when one abandons the network by sending a de- authentication, or deauth, message. An attacker is capable of sending this deauth message to an access point attached to client IP addresses. Table 1 displays the various types of attacksthat takes place on distinct SOA layers.

Table 1 Various SoA layer Attacks

Layers	**Attack type**	**Attack Mode**	**Attack Consequences**
Sensing Layer	Eaves dropping	The opponent tunes the specified frequency of the receiver's end	Receiver's private information are read by unintended attacker
	Jamming	The data packets are attacked by malicious node through notorious frequency	Averts response of valid data packets
	Active interference	Obstructs the communication network	Alters the message sequence
Network Layer	Black hole attack	False optimal route message	Damage to the private data on packet
	Rushing attack	Disrupts route detection progression	Forfeitures the safe route
Service Layer	Malicious code attack	Viruses and worms	Attacks OS functions
	Repudiation attack	Denying communication access	Communication failure

Interface Layer	Selfish misbehavior of nodes	Selfish nodes	Packet Dropping
	Malicious behavior of nodes	Interrupts routing protocol process	Misdirects traffic
	Traffic Analysis	Topology information	Information to inadvertent receiver

6 Tips to minimize IoT Security Vulnerabilities

There are ten suggestions proposed to minimize that security threats targeting the IoT enterprises thereby providing alertness and lessening controls to less-secured devices. The significant factors that helps in achieving a successful IoT security practice is having a sturdy understanding of the role of devices in the network, their controls and the security mechanisms involved.

- The password on every device must be reconstructed from default setup. If suppose, a device has fixed default password then use of such device must be omitted. The agreements of these password settings must be less nominal for proper functioning of devices.
- The network-oriented actions along with back-end or cloud service are to be properly explored before putting into production.
- In order to possibly protect unsecured devices from core networks and resources, it is necessary to have an isolated network behind a firewall along with vigilant monitoring of IoT devices.
- Avoid using unnecessary features like the OTA (over-the-air) where one must disconnect microphone when using a display only smart TV.
- Look out for physical compromise that results in vulnerability like a hardware “factory reset” control, open ports or default passwords.
- Avoid auto-connecting to open Wi-Fi networks as they result in security compromise making user data vulnerable to threats.
- If one cannot block all inbound traffic to IoT devices, they should ensure that there are no open software ports allowed for traffic flows.

- Encrypting IoT devices provides a phenomenal factor in protecting them during data transmission.

3 Social Media Security

1 Introduction to Social Media

Nowadays, social media plays a dominant role in the society. The resources that are used for accessing social media are computers, Smartphones, and other Internet connected devices. People with all ages possess these devices to interact with the outside world through various networking sites and pages. The main idea behind the social media is the platform that makes users to express their views and concerns regarding anything and sharing it with other people on the same platform. These also includes posting of photographs, videos, activities etc. They can reach any people near or farther away from their place. Despite providing all these advantages to individuals it is essential to observe the shared information is not as secured as one believes.

Certain users try to gain profit by exploiting another person's information. These acts include cyberbullying, harassment or cyber-stalking. These attacks are common threats to teenagers who continuously spend their time on social media with intent of becoming popular. They are often carried away by rumors spread by someone on the same platform. Hacking individual's account to post something illegal or inappropriate description of one is the common act in social media. This act during extreme situations has also forced victims to commit suicide. A ruthless exploiter uses social media by acting as a trusted person to connect and share thoughts with other persons and then harass them by cyberbullying them. Therefore, every individual before posting any information regarding oneself should be aware of the consequences.

Social media security discusses to the process of securing the powerful social media content from threats or issues that may be caused due to the attackers. Every organization at some point of time becomes victim to these issues that may result in any major or minor loss both to the organization or to the individuals present in it. Maintaining social media security for large enterprise networks is often defined as a critical process since it involves numerous factors. Some of the measures to ensure security are

preventing fraudulent from scams, phishing attacks or account compromise, protecting corporate accounts, and defending against various other attacks.

2 Crimes in Social Media

The practice of various social media applications such WhatsApp, Facebook and Twitter has gained much popularity in recent times altering the means of understanding and facing e-crimes and victimization. Formerly, people had an idea of social media crime based on the posts that were posted. In fact, the Social media has also designed new apprehensions associated with crime itself. The abuse encountered in social media platforms are not unusual. Therefore, Social media has initiated new prospects in solving crimes by the criminal justice agencies. Some of the most frequent crimes committed on, or because of social media are:

- Online Threats, Stalking, Cyberbullying
- Hacking and Fraud
- Buying Illegal Things
- Posting Videos of Criminal Activity
- Vacation Robberies

Figure 19 shows the frequent crimes that occur on social media.

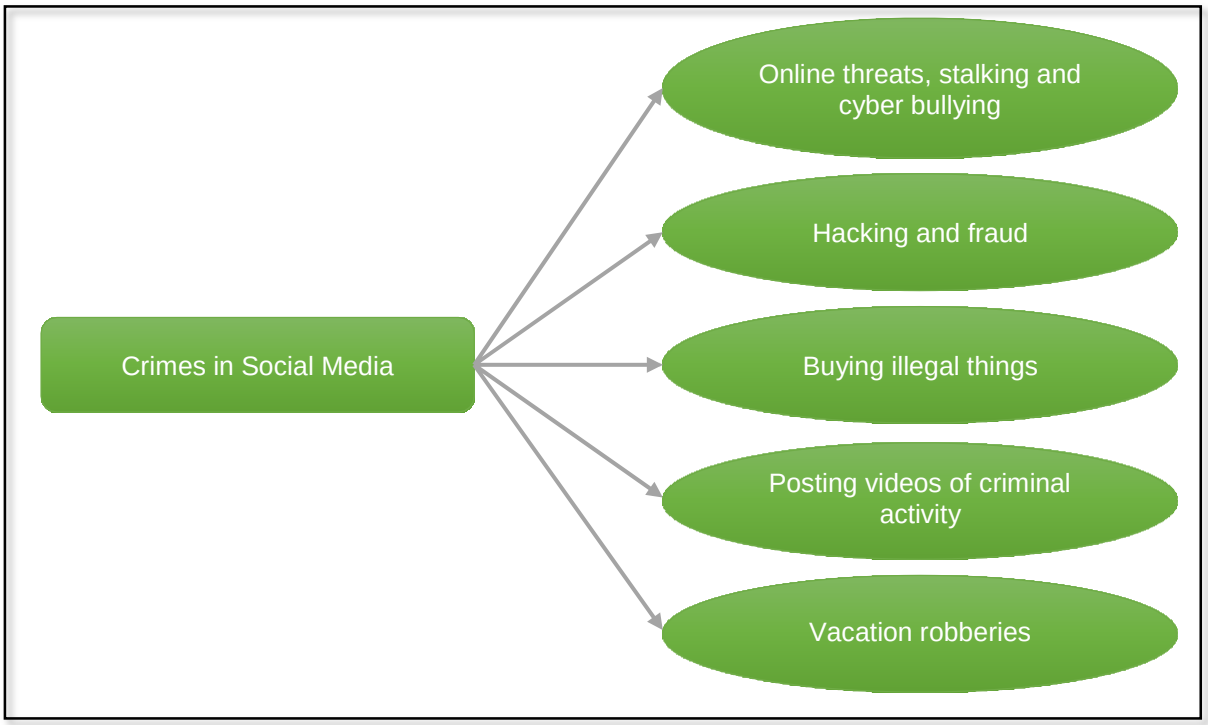

Figure 13 Frequent crimes in Social Media

1 Online Threats, Stalking, Cyberbullying

The predominant informed and perceived social media crimes includes threats, bullying, harassing, and stalking individuals online. Since most of the activities goes unaddressed or without charging of any penalty, victims of the crimes often be ignorant about reporting it to the officials.

2 Hacking and Fraud

Hacking refers to the process of illegally logging into another user account to perform ill-legitimate activities like embarrassing the users through awkward posts, generating counterfeit accounts, or impersonation accounts. The main purpose of hacking and fraud is to trick users and gain any kind of benefits showing that they operate from a legitimate identity.

3 Buying Illegal Things

The process of buying illegal things such as drugs, smuggled products, gold etc are punishable by law. These activities are now increasingly carried out through online social media.

4 Posting Videos of Criminal Activity

Due to the increasing usage of smartphone and digital technologies, most of the convicts post criminal video activities on social media. This creates shock among various users watching them but at the same time are useful for police divisions and lawyers to seize and imprison the offenders.

5 Vacation Robberies

Most of the users have a habit of posting all their daily personal activities on social media. Hence, burglars follow these type of users through their social media account and identify their vacation occasions to gain any monetary benefit.

With increasing developments in digital technology, social media has gained every positive and negative aspects related to criminal justice and law.

3 Common Social Media Security Risks

Some of the social media security risks that occur common can be listed as follows,

- Unattended social media accounts
- Human error,Third-party apps

- Phishing attacks and scams
- Imposter accounts
- Malware attacks and hacks
- Privacy settings
- Unsecured mobile phones

The common social media risks are displayed in figure 20.

Figure 14 Common Social Media Risks

1 Unattended social media accounts

Users who leave their social media accounts unattended for long period of time have more chances of being victims to attackers. Hackers collect all unattended reports of user accounts and choose one or some to post illegal or fraudulent messages in actual user name. Users who are present in the same platform consider these actions are carried out by the actual user. By this way, other users may also become victims to the attackers when they click or open any link posted from that account. The individual will be unaware of these activities until they are notified by customer help supporters.

2 Human error

This type of risk is very common. There are no perfect individuals each of them may commit mistakes unknowingly. Carelessness might lead to even large threats within the organization. Any inappropriate action may include simply downloading a dummy file

that contains virus or any other threats. A recent survey has proved that the major cause of cyber threats in an organization is due to the carelessness of the staff members.

3 Third-party apps

This type of risk happens when an individual purchases applications or services from third-party service providers. These apps are prone to vulnerabilities caused by attackers due to poor security measures. When user installs a third-party application then the work of a hacker becomes easy by intruding into the system through the security loopholes.

4 Phishing attacks and scams

Phishing attacks are very common. A fake email is sent in the name of a trusted user to perform actions such as clicking or downloading of a link or attachment. By this the attacker gains access to confidential data asking user to provide with details such as passwords, account numbers etc., These scams also redirect users to inappropriate Webpages posing them to several risks.

5 Imposter accounts

Imposter accounts are those that appear as trusted accounts for other users. The increase in the fraudulent accounts have raised over years. Attackers create these accounts unofficially to gain profit in some way or other by fake messages or calls. They request for user's confidential information in an official manner and exploit them even
without the knowledge of the user.

7.3.3.6 Malware attacks and hacks

At present, the hackers in social media have evolved world-wide. Hackers use a counterfeit profile to associate with workers of besieged administrations. By allocating a file with the invaders, they gain inaccessible entree to the target computer systems.

7.3.3.7 Privacy settings

Every individual experience both advantages and disadvantages of using social media to post privacy contents. Most of the users know that their data is not as protected as they think. The level of privacy in social media is considerably very poor. Despite knowing all these issues people still choose to use their own social sites of their interest. This privacy issue is generally a higher form of risk for organizational users where accessing social media is done for personal or business purposes.

8 Unsecured mobile phones

Mobile devices are the easy form of access to social networks. Using mobile data, a user can simply log on to any social network with a single click. If these devices are lost or being stolen without any proper security methods employed, it will result in undertaking of social accounts by the attacker. They easily gain access to the accounts on the devices with a single tap. They also perform phishing or malware attacks to other contacts on the devices. Hence, proper authentication mechanisms should be provided on individual's mobile phone for preventing from serious attacks.

7.3.4 Securing Social Media

Securing social media can be done only if the organizations continuously monitor for any new threats across the social networks. By examining continuously, the occurrence or instance of false interpretation of their organization then they are immediately reported and eradicated. With the help of this reporting process, the customers can be given an alert message through their official account in case of any serious threat issues identified.

One major attempt that helps to clear threat issues is by limiting publishing rights for users present in the social media channels. There should be distinguished rights between the user and the admin credentials. Every staff member should not be given access privileges to manage the account. A regular process of remedial connection is to be done in order to maintain a robust defense social media security strategy. A large interconnection of people may lead to large risk exposures. Hence social media security is a must in mitigating the risks that cause severe damages to the organization as well as
to an individual.

7.3.5 Social Media Security tips and best practices

Some of the social media security tips and best practices are:

- Generate a social media strategy
- Training individuals on social media security best practices
- Limit social media access
- Setup a system of approvals for social media posts
- Put someone incharge
- Keep track of accounts and involve in social listening

- Invest in security technology
- Accomplish a regular audit

The best social media security tips and practices are displayed in figure 2

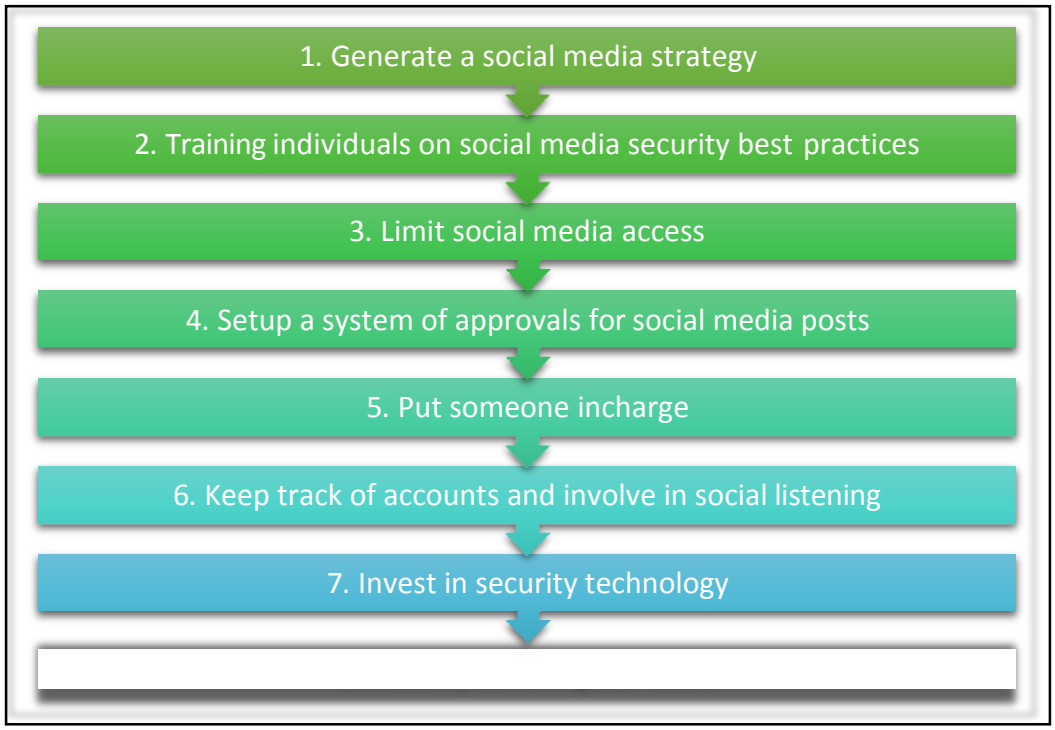

Figure 15 Best Social Media tips and practices

7.3.5.1 Generate a social media strategy

Every corporate organizations and employees are equally responsible in maintaining the security of their social media sites. For this purpose, they are assisted with various policies that protect them from various threat issues. These policies also help them from legal troubles and financial loss. Some of the social media policies that are assisted along with organization can be as follows,

- Explaining the company's brand on the social site with the help of some guidelines
- Ensuring the confidentiality of the personal use in the social media with the help of rules
- Identifying the social media account for responsible in charge of departments and the team members
- Confidentiality and copyright attested guidelines
- Rules for creating strong effective passwords and mandatory password change periodically

- Updating the software and services consistently
- Systems to identify and prevent security threats such as scams, phishing mails etc.,
- Generating notifications and responding to any new security concern identified

7.3.5.2 Training individuals on social media security best practices

A major cause of cyberthreat in social media arise due to the carelessness of the staff members. Hence the staff members are to be provided with proper educational practices on how to prevent themselves from being a cause to an attack. Even if organizations are provided with best security policies, they can be easily violated if employees do not pay attention to them. The training sessions help them with enough knowledge to pose questions in case of new security issue encountered. They are also provided with awareness training on current threat issues. Apart from educating the staff members suitable training tools are also equipped that helps them in overcoming the security issues.

3 Limit social media access

The threats to an organization's social media not only come from the outside world but also caused by the employees present inside them. The chances of employee exploitation are greater than a hacker exploit. This issue can be defeated by limiting access to the social accounts. An organization may have large number of people or teams managing the account in many forms such as messaging, post creation, or customer service. Hence, the admin is responsible to set access privileges by limiting users to post or make any modifications for security purposes.

The admin provides Hootsuite software for enabling right access to authorized employees. This is based on the idea admin creates account and no individual is prescribed with separate login information. When that individual resigns from the company then that particular account will be terminated without having burden to change passwords provided on the social network.

4 Set up a system of approvals for social posts

The owner of the organization is responsible to set up approvals for all the employees who are accessing the common social media account. By these approving methods, the users who can only the right access can post or make changes to that particular organization's account. Hootsuite is a tool that gives workforces or outworkers

the capability to draft posts and post them with a single press. But the final approval is given only by the reliable individual on the lineup.

5 Put someone in charge

Appointing a responsible individual as in charge of monitoring the social risks helps in minimizing the threats and issues. The responsibilities of this key person involve determining the users containing publish access rights, monitoring the presence of brand on the social site and the policies owned for security maintenance purposes. This person will be mostly the one who holds seniority in the marketing team maintaining a healthy relationship with company's IT department and play an important role in an organization's social media security development. This person also scans for members who might make mistake posing organization into risk that may vary from security issues to damaged reputations.

6 Keep track of accounts and involve in social listening

As stated earlier, social accounts that are unattended for long period of time become ripe for hacking. By continuous monitoring of social channels ranging from daily usage to subscribed but unused cases. Designating a person to keep track of the legitimate post on the accounts. Cross-referencing the posts against one's content calendar may be considered as primary step. Following on anything unexpected is necessary. Despite having the appearance of legitimate post, can contain serious issues too. It usually may be unsophisticated human error or large access gaining of individual's account. It is also important to watch for imposter accounts, any unwanted conversations about company's brand and untimely indications of organization's product by workers (or any allied person).

7 Invest in security technology

Even though the social channels are monitored by users that cannot be done all day long, software helps in those purposes. ZeroFOX are security software technology which automatically alerts of security risks. Hootsuite dashboard complemented with user integration of ZeroFOX helps in providing the following alerts,

- Alerts users of hazardous, hostile, or invasive contents aiming organization's product
- Notifies malevolent links displayed on social media

- Blocks scams that points the organizations and employees
- Identifies fake accounts imitating the product
- Provides protection against hacking and phishing outbreaks

8 Accomplish a regular audit

The evolution of social media has also paved way for many social media security threats that are inconsistent over time. this is because the attacker finds new technologies and implements them thereby affecting the individual or organization's social systems in the form of malwares or scams. Hence social media security measures are in the necessity to organize regular audits to stay ahead of the bad actors. Some of the audits that can be performed are displayed in figure 2

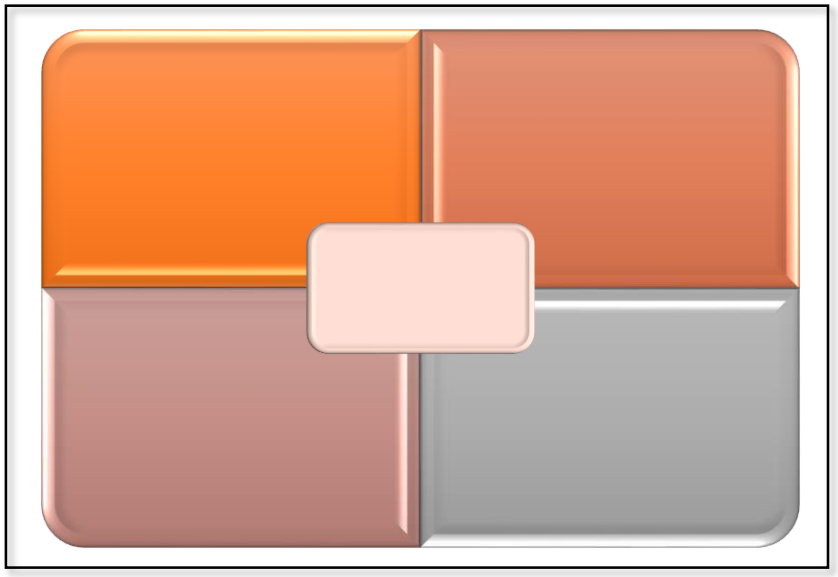

Figure 16 Performing Regular audits

- **Social network privacy settings –** Regular updating of the privacy policies in social media helps in ensuring security to user private accounts. These have impacts reflected on the account. For instance, a social network privacy settings update portrait the exact features of how user data control is maintained.
- **Access and publishing privileges –** The admin is responsible for monitoring the employees to whom the publishing right access has been given and also the power to update systems regularly. They also have the duty to check former employees access has been revoked and if there is any change in the employee role.
- **Recent social media security threats –** The organization in charge is responsible for maintaining a healthy relationship with the IT team to keep track and get notified

about new security threats. They are also responsible for collecting news regarding big hacks recognized by media.

- **Your social media policy –** A proper designing of social media security policy is must to prevent an organization from serious threats. Depending upon the inconsistent security practices, these policies should be modified simultaneously for ensuring security.

6 Social Media Security strategies

The social media security procedures emphases on providing a non-conceded security to the users. While designing these procedures, user must recognize the security area of concerns, ways to attain security, and persons in-charge of providing them. The procedure must also include areas that ranges from usage of social media applications to the user private terminals such as mobile devices, network security, and firewall boundaries.

The private network computer security is sustained by IT sector, responsible for granting or denying the capability to access features, possessions, and execute several activities. Since Public social media sites are outside to the organization's network, the control possibility are not extended to those locations.