Assessment of Cybersecurity Related Issues in Internet of Things

Arunabh Singh, Suraj Kumar Singh, Akhilesh Kumar, Krishna Gullapalli, Naveed Qadir &
Dr Vimlesh Singh
arunabh18singh@gmail.com
surajkumarsingh326@gmail.com
akhisingh1534@gmail.com
Krishnagullapali@gmail.com
naveedqadir0@gmail.com
vimlesh.fet@mriu.edu.in
Electronics & Communication Engineering, FET, MRIIRS, Haryana, India

Abstract: This paper is presenting issues related to Cybercrimes and data breaches in automation system. Issues and data security in IoT devices are address in this paper. Need of fixation of the defensive mechanisms at frame work level incorporated. Hardware based system issues of the devices and equipments change with networking technologies. Assessment and challenges of cyber security in smart devices and smart machinery is discussed. Recent developments in IOT as well as few substantial cases of security breach in the past decade also presented in paper. This paper also covers the various issues and liabilities that still exist within industrial and residential region by analyzing the statistical data surveyed in the past few years.

Keywords: Cyber security, Industrial IOT, Consumers, Home automations, Healthcare

1. Introduction

Internet of things (IoT) is Encompass of interconnecting computing devices like electronic system, object, Living organism which had capability to transmit information via network without the need of human or human-to-machine interaction. It is a technology that merge the large number of electronic devices together via online modes of communication. IOT makes like easy and comfortable but it also arises certain challenges like Cyber security and privacy concerns. Cyber security and privacy related to data are most significant challenge for private and public organizations. Any open end in system framework of an IOT system could be the reason of cyber security attack. These open ends are because of the interconnectivity of networks in IOT which enables intrusion from unknown and suspicious sources. It is quite unfortunate that the users often don’t have the required knowledge of the security management until there is a breach in the system, causing substantial damages such as loss of sensitive data. With the current situation of security breaches that have endangered the privacy of users, the appetite for IOT based technology within competent threat management systems is declining. The distinctive features of IOT devices had potential to make the pre-existing network framework more significant and feasible towards defensive mechanism. Even then, IoT devices might not be able to protect themselves from hackers because of inadequate computing resources as well as less security expertise from consumer and manufacturer end[1-3]. It is the network which the core of infrastructure responsible for inter linking smart devices with each other and on other hand connect with Internet and cloud to stores and assess this data. The significance of the network creates opportunities for new research based on inconsistency and error detection which also includes intrusion deterrence and device access control mechanisms, so that the network can prohibit undesired traffic and detect suspicious activity. While these are quite significant issues in network security, IoT helps in providing new opportunities for their rectification. Most of the IoT devices have a constricted agenda which are explain in this paper as example like picture frame that exhibits photos gathered on specific cloud platforms which eventually create unique traffic configurations to enable various ways of detecting glitches and errors. The massive technological developments in IoT has aided organizations in various ways including market research and business strategies. IoT system enhanced the socio economic status of individuals by establishing automated services. These development also increased security threats to the users. The careless use of smart devices, unauthorized cookie settings, and the lack of knowledge about security settings and updates have increased cyber security risks and enabled access to malicious applications and software’s put sensitive data at risk. Improper security practices by the users increase the chances of a data breach and data leakage. The professionals believe that IoT system could be a soft target for cyber attacks due to inappropriate security protocols and policies to use of IOT system. Hackers have initiated varying kinds of malware to infect IoT devices since 2005. If device manufacturers and security experts analyze the cyber threats correctly, they can create an efficient protective mechanism to avoid or nullify cyber threats. IoT systems have considerable security requirements and removal of malpractices. An Thus, it is important to hire professionals who are capable of dealing with such issues and also develop diversified security measures and policies to safeguard business assets and make sure that services are easy to access and completely secured. The recent developments in the 5G network, going to have an essential role to play in the IoT applications and devices like smart phones and smart watches. But along with it 5G is also attracting more and more security and privacy risks as stated by researchers, all due to its properties like high frequency and bandwidth. Since the short wavelength necessitates big changes in the infrastructure, thus there is need of several new base stations to traverse greater area as compared to other wireless technologies. IoT system consist of five layer system[14-16] architecture for layer level security of the system as shown in figure A.

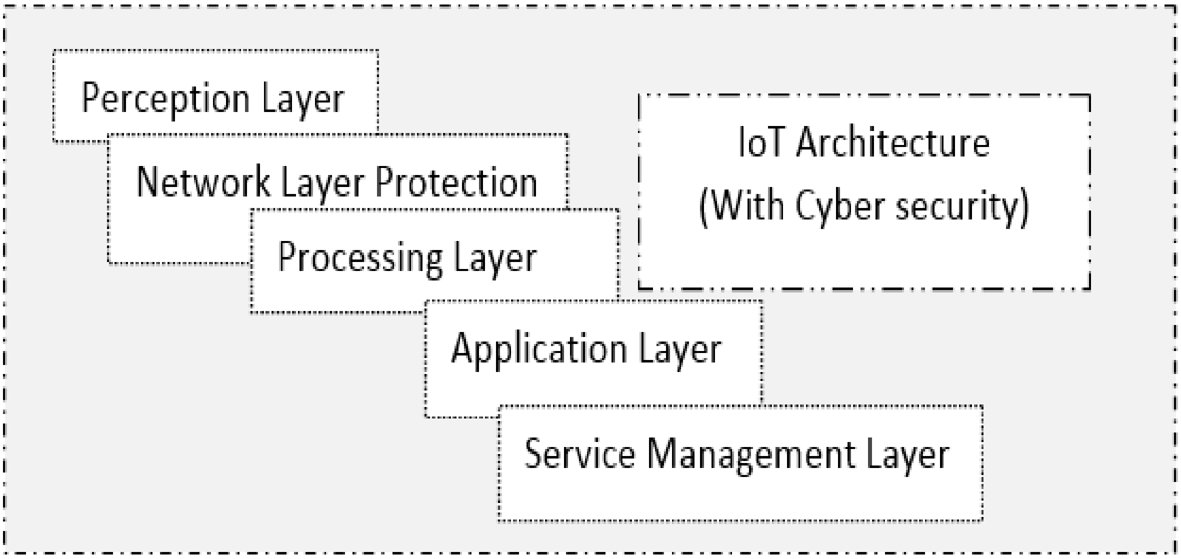


Figure A: Cyber security in IOT System [16]

This also gives rise to new threats, like fake base stations. Several law enforcement agencies are making consumers aware about the dangers of carelessly embracing IoT technology without prior knowledge of its risks and liabilities. Recently FBI made an announcement which suggested that consumers should operate IoT devices with their own protected network and they should be aware of the threats imposed by these devices. The security issues are further enhanced by the fact that several IoT devices might be built by companies that have little or no expertise in cyber security management. IoT devices had constrained in term of hardware at preparation layer due to cloning of chips used in system, is major security threat [16-17]. To avoid cloning issue it is necessary to use system cryptographic key for identification & authentication of chip [13-14]. Certification of complex framework of an IoT device in term of security is difficult in respect to legal and technical prospect [15]. At network layer secure transmission of data is the major task. At this level an threat detection system needed for, monitoring and correcting the system [5] [7-8]. As a security measure protocol verification is added at this level for identification of suspicious behavior of system. In processing layer data is streamlined. For this level various data clouds for data processing. At application level data monitored, controlled & analyzed for various IoT applications [9]. In service management layer, security focuses on organizational level and personal level.

2. Cyber security in Industrial Internet of Things

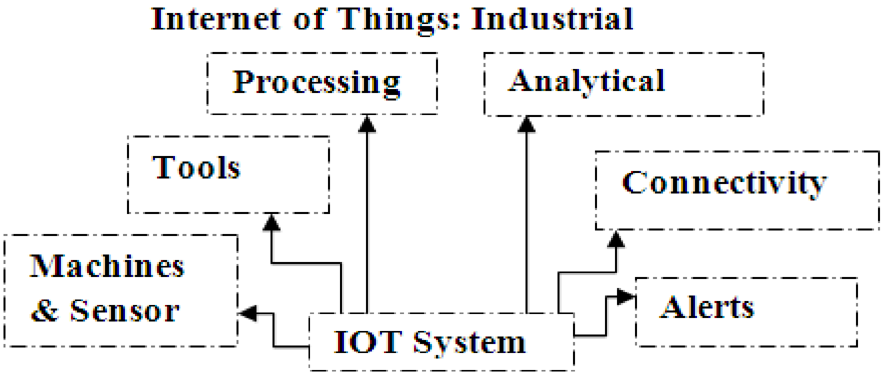


Figure B: Various aspects of IIOT

To accomplish effective and supple production at reasonable cost, industrial automation is driven towards digitalization. To meet the goal of industry it is necessary to add automated control system for high quality and bulk production. Industrial IOT system delivers an encouraging prospect to design and execution of compelling industrial process. Numerous industrial IoT based applications have been implemented.

Inclination to adopt IoT based industrial process is increased now a days. The implementation of IoT systems in different domain of society like security surveillance, processing industry, agronomy, food production and security, various types of pollution monitoring system, and may more. The manufacturing industry is traversing through a swift evolution which has been fueled by the Internet connectivity technologies like Zigbee, 6LOWPANetc. The standardized shift of production industries called as Industry 4.0 in western countries except for USA where it is termed as Industrial Internet. It is a popular belief that a constantly evolving Industrial IOT will deliver optimization and cost-saving by smart production in different industrial sector. A recent report of Industrial Internet Consortium (IIC), states that IIOT system will facilitate substantial advances in optimization of decision-making, production procedures and alliances with large number of autonomous control systems. Use of Big-data in industrial application help in decision making towards smart production. As per International Electrotechnical Commission (IEC) the basic utility of Industrial IOT is to empower support and cooperation within devices. The precise execution of cyber security in an Industrial IOT system will be one of the dynamic factors for its progress, thus amplifying its credibility in various attributes like quality and veracity of data, asset accessibility, etc. However, several of the devices in an IIOT system will be resource constrained with respect to computational capacity, network bandwidth, etc., simultaneously there might be practical needs and demands on signal handling. This blend of limitations and needs generates distinctive challenges associated with , while the classical cryptographic procedure simplify the workload on both the network and CPU operation. IIOT systems interlinks and incorporates industrial control mechanisms with enterprise structures, business procedures and analytics[4-7]. This definition accentuates IIOT as a mode for boosting whole production worth.

Some of the significant security breaches in IIOT sector of industries are stated below:-

- ***Duqu:-*** It searches for data which is useful for an ICS attack by manipulating a zero-day liability in Microsoft Windows systems.
- ***Havex:-*** A remote access tool(RAT) employed for attacks against several industrial targets, especially the power sector.
- ***Stuxnet:-*** Manipulated 4 zero day liabilities developed to infect industrial programmable logic controllers(PLCs).
- ***Black Energy:-*** Utilized in a complex movement to focus on ICS systems operating an industrial organization’s human to machine interface merchandise.
- ***Triton:-*** Exploited a zero-day liability in a big electric company’s Tricon safety system firmware.

It so happens that various reference architectures associated with IIOT, the most significant ones are:- “Reference Architecture Module for Industry, 4.0”recommended by IEC and Industrial Internet of Things Infrastructure recommended by the IIC. For sizable amount of IIOT applications, the intricacy of the data substructure depends on:

- **Size of structures**
- **Complex devices**
- **Device-to-Cloud Sequences**
- **Miscellaneous technologies**
- **Numerous shareholders**

This implies that IIOT can also increase the risk of potential cyber attacks and losses on multiple fronts. Cyber criminals, competing rivals, countries involved in corporate reconnaissance or even discontented employees can cause damage to the company because of which its losses can increase at an incalculable rate.

3. Cyber security in Consumer IOT

Consumer IOT covers varying amounts of consumer wearable’s and consumer IOT systems which have specified functions and purposes. Consumer IOT in itself does not have a well defined meaning but we can elaborate it by taking into consideration the various sectors in which consumer IOT based devices have contributed to the facilitation of consumers. Some of these smart devices fall into the following categories:-

3.1 Home automations: Smart devices of a connected home

It is quite impossible to ignore the issue of cyber security with respect to the growing importance and demand of smart devices in the residential sector i.e. Connected homes. These smart devices also known as home automations are comparatively more feasible with excellent storage and connectivity capabilities. Also, their definition is not restricted to smartphones and smart watches but all other sorts of appliances which can be interlinked with each other with the connectivity technologies IOT, some of these device include smart air conditioners, smart washing machine, smart security system, smart TVs etc. Although this provides many benefits to people who work with home automations, it also makes security breach inevitable. Thus, we must ensure that appropriate measures and steps are taken to safeguard the vulnerabilities[10-11]. Some of the important smart devices and systems that are interlinked in a connected home are mentioned in figure C

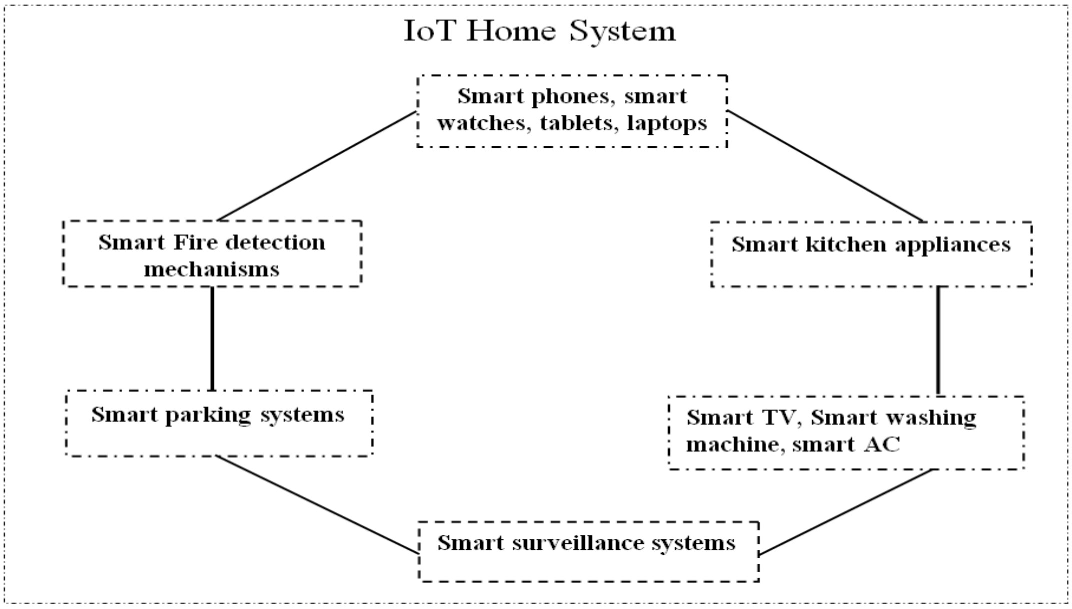

IoT Home System
Smart phones, smart watches, tablets, laptops
Smart Fire detection mechanisms
Smart kitchen appliances
Smart parking systems
Smart TV, Smart washing machine, smart AC
Smart surveillance systems

Figure C: Connected home

Use of smart devices in smart environments produces an incalculable amount of data, often without the assent of the consumer, or without the user being fully aware of the consequences of sharing their personal data by working with these devices. Hence, in some cases, a user friendly approach must be opted for designing networks which are capable of facilitating users involvement and command wherever required. They envisioned the personal network as a dynamic extension of the PAN(Personal Area Network) to encompass the user's home network as well as networks such as a VAN(Vehicular Area Network). A recent example of the implementation of a PN is the EU-FP7(European Union-Seventh Framework Programme) research project, "Webinos". The main purpose of this project is to create personal networks that traverse through the PAN, residential and automobile environments as well as cloud-based platforms. These smart devices are suspected to have stored a large amount of confidential data which is generally used in online transactions and for other important purposes. The use of easy to access smart device platforms like IOS and other third-party applications delivers greater opportunities for hackers and cyber criminals[12]. Therefore, in the coming decade smart devices will become some of the most beneficial targets for cybercrimes. People are vulnerable to easily downloading malware in their smart devices and fall prey to their cyber-attacks where hackers masquerade as legitimate entities in order to seize and alter sensitive data, and then make use of it for ill purposes like cyber bulling, data thefts and data corruption. Thus we can say that the most vulnerable link in an IT security chain is the user.

Service providers, and hardware retailers must be aware of their duty to maintain network security and data management in the devices and other electronic equipments they provide. Service providers are also capable of providing additional security services to monitor the vulnerabilities of smart devices. Approximately eight in ten people, report they use their smart phones to store and utilize sensitive information. Juniper Networks Mobile Threat Centre (MTC) reported that in 2011 there was an massive increase of mobile malware attacks as there was an increase of 154%attacks as compared to 2010with reference to several IOT platforms. We can say that devices such as smart TVs, smart kitchen appliances and smart meters are quite exposed and incompetent to facing threats and intrusion from unlawful sources. IOS based devices suffered from even a greater number of cybercriminal attacks due to their increase in demand and exposure to cyber threats, even the world famous hacker groups such as the Anonymous are known to target these vulnerable sources. Thus we can say that smart devices especially home automations pose a bigger threat to smart environments that protect highly sensitive data which can lead to the targeting of individuals for several political and financial causes. Device connected to the web can take several forms, ranging from primitive devices that determine things like temperature to complex devices like video cameras that record and survey the physical activities of anything from homes, streets to secluded oil refineries. These devices are quite prone to security breaches they operate on unprotected networks. Apart from this the greatest problem of devices interlinked with IOT is that these smart devices get exposed to various layers of Internet i.e. the surface net and the dark net. Now, most of the users usually work on the surface web and lack knowledge about the functioning of dark net but hackers, cyber bullies and other network specialists have various access points to infiltrate smart devices like smart phones and extract personal information.

They are able to commit such deeds with the help of dark net which includes controversial search engines like Shodan. These search engines provide access to various smart devices across the globe without the users knowledge. The internet is basically an ocean of knowledge and data which is being transmitted, generated and streamed online by incalculable sources. Consumer IOT may have helped people in making their day-to-day lives easier but along with it they have also placed their private lives in the grave peril as the information regarding their personal activities and requirements is now being stored on social media and other easy to access platforms, all thanks to the internet. In past few years, work has been done to protect computer servers and networks from malevolent attacks, but the emergence of home automations has forced cyber-security analysts to revise their strategies for protecting network integrity and the respective users from exploitation. One of the major strategies for defensive control systems is to separate personal networks from other networks. Since the control systems are now connected to the Internet that approach will hardly work as efficiently as it did before. Thus, there's a vital need for multi-layered user friendly security system i.e. merging precautions for certain devices, servers, networks and applications with more powerful access control mechanisms, data management and network supervision[18-19].

3.2 Healthcare Devices

Healthcare is one of major area where IoT can bring revolution to provide facilities to rural population. Basic & advanced applications connected with IoT services can cater patient, doctor and caretakers in healthcare sector. The IoT is being revolutionised for the purpose of recreating contemporary health care services with feasible economic and social outlooks. Hospitals are also using IoT to supply practically accessible health care facilities and also to store and utilize the data of their patients and staff. There are several mobile applications and consumer wearable's which allow patients to record and assess their health data.Some of these applications with enhancement by 5G technology is explained in figure 5.

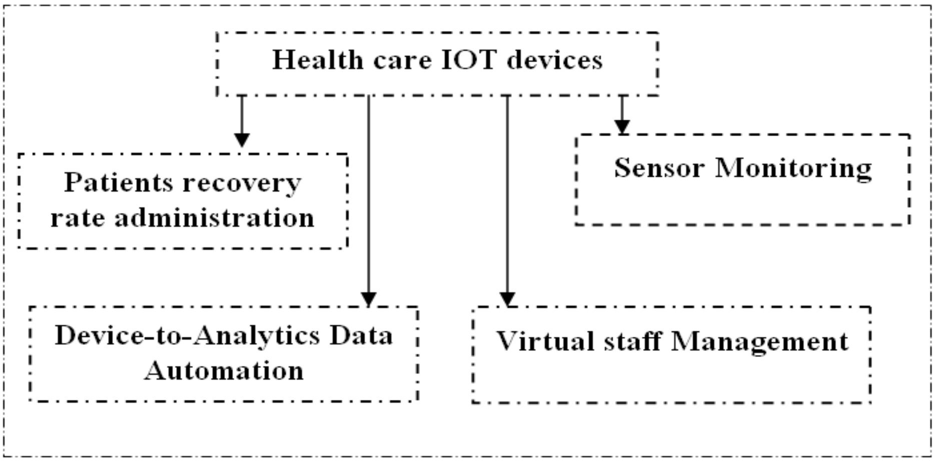

Health care IOT devices
Patients recovery rate administration
Sensor Monitoring
Device-to-Analytics Data Automation
Virtual staff Management

Figure 5: Applications of IOT in Healthcare

Hospitals are also using IoT to supply practically accessible health care facilities and also to store and utilize the data of their patients and staff. Many of the IoT healthcare devices and applications are capable of monitoring different health attributes which include blood pressure, blood sugar level, cardiac fitness and weight management etc. IOT has the capability to keep a precise record of patients, devices, samples, resources, medicine and assess the data recorded. Various types of devices combining with impromptu networks and sensors are established with IOT to assist patients and doctors in several important services. As patients are connected to sensors to record and assess important recovery statistics and other biometric data, problems might be diagnosed comparatively earlier, thus, a much better quality of Health care services can be provided. Although these applications may sound exhilarating but practically feasible mechanisms for such systems have yet to be constructed, and for their accomplishment several barriers must be tackled. These barriers exist due to technical issues, safety of patients and staff, security, privacy and data breaches. Healthcare organizations must enable balanced and carefully surveyed infrastructures to ensure that the benefits of smart devices without increasing an excessive amount of risks to the health and well being of patients. Healthcare workers and patients are introducing more and more smart devices into healthcare networks. Over the past eight years, IoT technology has enhanced the performance and the functionality of hospitals and nursing homes, but its growth has also provoked a steep rise in cyber security related threats.

These smart devices are utilized for patient monitoring, asset tracking to assist health care workers in more easily finding equipment's and computerizing HVAC(Heating, Ventilation and Air conditioning) systems . All these advantages of connected medical devices can simplify and rationalize workflows that further enhance the lives of patients and professionals like surgeons, radiologists, forensics and staff members but they also lead to increasing the opportunities and ease of conducting illegal activities for cybercriminals. Many considerable breaches over the past decade have shown the urgency of growing medical cyber threats and have in turn compelled manufacturers, and several healthcare organizations to place more emphasis on healthcare IoT Cyber security[14,18-19]. In 2016, security research organization Med Sec and financing company Muddy Waters Research identified a liability within a specific St. Jude Medical cardiac device, where an attacker can easily send pirated messages to the device so as to drain its power and reduce its efficiency. At Black Hat 2018, many researchers disclosed substantial insecurities in medical IoT systems. Along With them, researchers Billy Rios, founding father of White Scope security firm, and Jonathan Butts, Chief executive officer of QED Secure Solutions, proved how hackers are able to infiltrate a Medtronic pacemaker with ease and regulate shocks to patients. WannaCry ransomware is amongst the foremost renowned cyber attacks which was responsible for targeting major healthcare systems and devices, beginning from 2017. Hackers operated WannaCry to access the vulnerable links within the Windows OS and barred the healthcare authorities from recognizing and retrieving the corrupted devices. In 2016 and 2018, the FDA issued post-market and premarket cyber security proposals for manufacturers to design and maintain frameworks for uplifting healthcare IoT security. Organizations that acquire medical devices for healthcare facilities, like HealthTrust and Mayo Clinic, also launched their own prerequisites for medical smart devices . These requirements forced manufacturers to enhance security systems in their products. Manufacturers devote money where there's significant need or demand or significant opportunity for gaining profit and therefore the cost of recovering from the damages are going to be heavier as compared to preventing the damages. Healthcare IoT Cyber security issues depict a more serious challenges than the issues present in smart home devices because if healthcare devices malfunction then might cause physical harm. Healthcare professionals and patients rely on precise information with 100% accuracy to make decisions and oversee treatment during emergency.

With rapid developments in IoT technology, latest devices become available periodically and IT administrators may find it difficult to keep an updated account of liabilities and risks. Devices quite capable of joining a network in form of business initiative without the involvement of IT industry, which makes device detection crucial for IoT Cyber security. Operational technology (OT) specialists usually do not list out most efficient measures for security management and IT specialists are often unable to recognize security practices which are at risk of hindering various procedures.Thus it's important to have both IT and non-IT workforce at the field for the creation of desired mechanism to ease the workloads of security specialists. Legalized equipment might pose a security challenge when it is interlinked with the local network. In several healthcare organizations, devices and machines that are multimillion-dollar investments do not get modified or redesigned until they are completely useless or out of demand. Connecting these devices and machines creates liabilities. Thus it is possible the legalized equipment may not follow necessary protocols.To resolve these issues Cyber security professionals can opt for several preventive measures toenhance healthcare IoT security, some of these measures are as follows:

- ***Catalogue devices*****:** Design a thorough plan of all available assets. Since healthcare organizations are in competent in protecting devices which cannot be visualised, many IoT devices are bought or provided without an effective risk assessment mechanism as organizations are more focused on their features and value in market. For instance, a patient brought an “Alexa virtual assistant”(it is developed by Amazon in correspondence with Amazon Echo and Amazon Echo Dot) for the purpose of listening to music or some other form of entertainment, but there several vulnerabilities in the device due to its exposure to eavesdropping hackers who can easily gain access to its core system and induce malware and data intrusion. Just like the case with Amazon Alexa, There are several other e-health monitoring devices which should be assessed with caution and considerable security frameworks

- ***Adhere to standardised procedures:***Professionals should adhere to authorized security procedures for healthcare IoT devices, such as heavily coded passwords, firewalls settings and encryption. They should do a threat analysis before they execute devices to recognize the liabilities that exist within and supervise network traffic for unlawful activities using behavioural analytics profiling. Devices and software must be updated periodically.

- ***Execute efficient validation:*** Implementing publicised vital infrastructure and digital certificates can validate connections with the network, devices and the electronic healthcare data analysis mechanisms, and guarantee that data packets are not altered or manipulated while in transition i.e. from man-in-the-middle attacks.

- ***Segmented networks:*** Administrators will have to protect devices that do not possess built-in mechanisms for regulating data management and its security. When a device is operated for nursing of patients, administrators can restrict its connectivity with the internet. If it is eessential for the device to connect, healthcare organizations could cooperate with the vendor to pin point the regions where the device must connect and permit only those connections, creating an permit list.

- ***Usage of appropriate equipments*****:**Healthcare organizations can utilize equipment’s which are able to streamline IoT security. There are some selective platforms which are capable of computerizing the management of large amounts of information and devices. Besides this, they are also able access control over the authentication certificates. Manufacturers have also initiated medical device apparatuses that can recognize the basic functions of a device, the different kinds of data collected it collects and the points where it is connected to the internet.

There are some major devices that have boosted the growth of IOT in healthcare sector but along with they have also arisen certain issues that are threatening to expose the healthcare[12].

4. Risk Management

The risks also comprise of equipment failure, loss of crucial data and corporate image, and even harm to life. IIOT technologies can improve operational efficiencies to a great extent, yet they are also exposed to potentially new attack surfaces and security liabilities if not properly protected from Cyber intrusion. Each and every machine joins "a system of systems" as it gets interlinked with more and more IIOT devices. Technological developments like 5G will most likely boost the usage of IIOT machineries by supporting the infrastructure required to hold massive amounts of data. But this also increases the attack surface. Practically, anything and everything is at the risk of becoming vulnerable i.e. from valuable assets or services, crucial projects and tasks assigned in the cloud, process controlling subsystems in cyber-physical systems to confidential business and operational data[16-18].

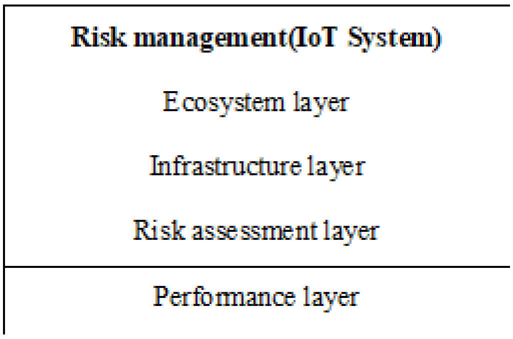
There two major approach for management of cyber risk in IoT system:

1.Qualiative Approach

2.Quantitative Approach

For instance, if an electronics manufacturer uses Safety Instrumented System (SIS) controllers to analyze data from industrial equipment systems so as to provide aid to the management and functioning of machineries. Iterations to these systems may cause physical damage and interrupt operations. Electronics manufacturers are at high risk of exposing automated equipment and computerized processes to adverse Cyber attacks and their consequences this come in qualitative approach. Four layer cyber security management system is one of technique which provide effective solution to risk management in IoT system. When this data is assessed, it provides companies and organizations a clear understanding of their manufacturing procedures and creates several new business and production opportunities. Organizations require there sources which will contribute in protecting their assets and networks, along with their whole IIOT ecosystems.To thoroughly understand IIOT security risks and its repercussions, the IBM Institute for Business Value (IBV) affiliated with Oxford Economics to survey about 700 executives. Automation of machinery and manufacturing procedures are also very common applications, with about 46 percent of surveyed organizations using IIOT technologies to automate equipment and administrative systems.

Table 1. The Four layers of Risk Management



Risk management(IoT System)
Ecosystem layer
Infrastructure layer
Risk assessment layer
Performance layer

Electronics companies are conscious about cyber security related liabilities and are constantly working to cope with their security expenditure. Amidst the rapid embracing of latest IIOT based technology, companies which are not adopting relevant cyber security protection measures, are at exposure to several significant risks:

- ***Leakage of confidential data:***-Examined executives address this as their greatest risk. Sixty-five to seventy percent are acutely aware of the extent to which exposure of such confidential and crucial data, such as client and staff information, broker and business partner intellectual property and agreements, would impact on their company's economic and financial growth.

- ***Harming of an organization's reputation and loss of public faith*:-** The adverse impact to an electronics company's name and status, subsequent of security breach could be massive. This has been stated by55-60 percent of executives. The integrity and honesty of a brand can be destabilized along with businessmen and client relationships damaged beyond repair.

- ***Interruptions in production as a result of sabotage***:-Forty-five to fifty percent of executives have stated that this type of risk is substantial i.e. it has the potential to damage electronic and mechanical equipment and also cause injuries to worker sand employees responsible for the production of goods and services.

- ***Intellectual property (IP) theft:-*** IP is vital for the company's future development. Trading secrets, like for instance engineering models and patented manufacturing procedures, are sources of economic benefits. Forty five percent of electronics companies have identified the impact that IP theft could produce on their future development and growth.
- ***Infringement of supervisory requirements:-***The General Data Protection Regulation (GDPR), active since May 2018, combined with environmental laws administering products and production procedures, amplify supervisory exposure and risks. Thirty-five to thirty-eight percent of examined executives are extremely worried about the impact of nonconformity with supervisory obligations i.e. violations that can lead to significant penalties.

Security mechanization refers to facilitating security frameworks and system models so as to strengthen or substitute human interference in the recognition and restriction of cyber security threats or breaches. Such models rely upon artificial intelligence(AI), machine learning, business analytics and instrumentation. While attending to these issues we recommend some precautionary measures and safeguards that can help in solving security related issues in IIOT. They are as follows:-

- ***Establish IIOT user privacy control mechanisms:-*** If consumption data can be inter linked with devices, information about a company's progress and manufacturing secrets can be easily determined. To tackle this, companies must establish control mechanisms which permit users to stipulate how data is collected on their devices and how it is transmitted and utilized by third parties.
- ***Establish IIOT authentication mechanisms for user verification:-***A large number of companies are in the advanced stages of implementing this procedure. The capability to validate IIOT device individuality is highly important, particularly for IIOT machine-to- machine (M2M) settings in which devices are often neglected.
- ***Elaborate thoroughly the service-level agreements (SLAs) for security:-*** Almost three fourth companies of the world supervise and impose security obligations this way. To battle inner threats and attacks, and prevent information theft or manipulation, establish regulated access to data.
- ***Implement IIOT devices which possess built-in diagnostics:-***Many companies are executing devices that identify malfunctioning of the system caused by inadequate functionality of components or attempts of rigging. IIOT terminuses must often function in harsh environments without human involvement for long intervals of time.
- ***Computerize the scanning of connected devices:-*** The practice of incessant vulnerability analysis and remediation is critical. Execution of dynamic vulnerability scanning can unfavourably affect ICS network communications and also product and system accessibility.
- ***Install secure and toughened device hardware and firmware:-***Substituting devices is quite costly. Also, latest devices may not be accessible with enhanced security. Companies should regularly perform synchronized patching and updates, despite the intrinsic challenges of updating devices that often operate throughout the day, and each and every day.

So, it is important to monitor various versions of softwares that boost the functioning and development of IIOT hardware components Also, we must care fully evaluate the risks related with modification and creation of regulated frameworks of IIOT for preventing security breach. These initiatives must be accompanied by a thorough understanding of endpoints i.e. agendas and means of communication. Each endpoint must be outlined and improved for asset accounting and supervision.

5. Conclusion

In todays senior IoT is basic component for smart cities, smart health, smart grids, driverless driving, smart manufacturing and many more. As the number devices and variety increases into the IoT system security related issues grow exponentially. Any short coming in the IoT systems give opportunities to hackers. This issue motivate cyber experts to find out a suitable risk management system for IoT. This paper reviewed the cyber threats in smart home, industrial & health care IoT based application. Paper contributing in assessment of risk in IoT system also describe the available frame work.

References

[1] Zanella, A., Bui, N., Castellani, A., Vangelista L.& Zorzi, M. (2004). "Internet of Things for Smart Cities," in *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32.

[2] Kumar, J. S., &Patel, D. R. (2014).“A survey oninternet of things: Security and privacy issues,” International Journal of ComputerApplications, published by Foundation of Computer Science, vol. 90, no. 11, pp. 20–26 .

[3] Laplante, P. A.,& Laplante, N. L.(2015)."A Structured approach for describing healthcare applications for the Internet of Things," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 621- 625.

[4] Ali, N. A., & Abu-Elkheir, M. (2015). "Internet of nano-things healthcare applications: Requirements, opportunities, and challenges," *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp.9-14.

[5] Kamilaris, A.& Pitsillides, A. (2016). "Mobile Phone Computing and the Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 885-898.

[6] Laplante, P. A.&Laplante, N. (2016). "The Internet of Things in Healthcare: Potential Applications and Challenges," in *IT Professional*, vol. 18, no. 3, pp. 2-4.

[7] Corno, F., De Russis, L.& Roffarello, A. M. (2016). “A Healthcare Support System for Assisted Living Facilities: An IoT Solution,” in Proceedings of the 2016 *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC),* pp.344-352.

[8] Menon, V. G.,&Pathrose, J. P. (2016). “Analysing the Behaviour and Performance of Opportunistic Routing Protocols in Highly Mobile Wireless Ad Hoc Networks", *International Journal of Engineering and Technology*, vol. 8, no. 5, pp. 1916-1924.

[9] Menon V. G., Pathrose J, P.& Vijay, A.(2016). “Eliminating Redundant Relaying of Data Packets for Efficient Opportunistic Routing in Dynamic Wireless Ad Hoc Networks”,*Asian Journal of Information Technology*,vol. 15, no.20.

[10] Menon, V. G.,& Pathrose J.P.(2016). “Routing in Highly Dynamic Ad Hoc Networks: Issues and Challenges”, *International Journal of Computer Science and Engineering*”, vol.8, no. 4, pp.112-116.

[11] Menon V. G.&Pathrose J. P. (2016). “Opportunistic routing with virtual coordinates to handle communication voids in mobile ad hoc networks,” in *Advances in Signal Processing and Intelligent Recognition Systems*, vol. 425 of *Advances in Intelligent Systems and Computing*, pp. 323– 334, Springer International.

[12] Menon, V. G., Pathrose, J. P.& Jogi Priya, “Ensuring ReliableCommunication in Disaster Recovery Operations with Reliable Routing Technique,” *Mobile Information Systems*, vol. 2016, Article ID 9141329, 2016.

[13] Bendavid, Y., Bagheri, N., Safkhani, M.&Rostampour, S. (2018). “IoT Device Security: Challenging “A LightweightRFID Mutual Authentication Protocol Based on Physical Unclonable Function”. pp.4354-4444.

[14] Mollah, M.B., Azad, M.A.&Vasilakos, A., (2017). “Security and privacy challenges in mobile cloud computing: Survey and way ahead”. pp. 38–54. [CrossRef]

[15] Xu, H., Ding, J., Li, P., Zhu, F.&Wang, R.(2018). “A lightweight RFID mutual authentication protocol based on physical unclonable function”. pp. 710-760. [CrossRef]

[16] Zhu, F., Li, P., Xu, H.&Wang, R. (2019).“A lightweight RFID mutual authentication protocol with PUF”. pp. 2889-2957. [CrossRef] [PubMed]

[17] Boeckl, K.R., Fagan, M.J., Fisher, W.J., Lefkovitz, N.B., Megas, K.N., Nadeau, E.M., Piccarreta B.M., O’Rourke, D.G.& Scarfone, K.A. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228. 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.