Information system for managers

1) The internet of things (IoT) has taken over homes and offices. In the medical industry, though, it takes on an all-new importance. Medical devices that are connected to the internet can gather data that can detect and diagnose issues early, possibly saving lives. This new approach to healthcare brings elevated challenges to cybersecurity teams. There are currently an estimated 30 billion connected IoT devices. The healthcare sector's usage of IoT devices is expected to grow to 162 million by the end of 2020, and each of those devices have to be tracked and catalogued by security teams. If a security breach is detected on one device, it could signal a way into the network for a hacker trying to gather patient data.Exabeam's analytics solution is built to tackle those challenges, automatically detecting activity on all connected devices and monitoring them. As new devices are added, the solution begins monitoring, learning typical behaviors through machine learning in order to immediately alert analysts when unusual activity is detected. Protecting patient medical, insurance and personal information must be a top priority. However, to best protect that data, security professionals need a better understanding of the types of cyber threats they are dealing with. The Internet of Things (IoT) refers to devices connected over a network. This network allows devices to share data and lets users monitor or operate them remotely. Smart TVs, watches and cars that connect to the internet are all examples of IoT technology. Creative digital agencies are speeding along the process, combining new technologies with successful app designs. Digital health care applications allow patients to plan their appointments without having to wait for a receptionist and call to doctor's office. Also, it allows doctors to transfer information with patients through smartphones. Let us discuss about IoT healthcare companies in India. In recent years, there has been limited growth in the Indian healthcare sector with the country lagging behind in many health indicators. Data security & privacy

One of the most significant threats that IoT poses is of data security & privacy. IoT devices capture and transmit data in real-time. However, most of the IoT devices lack data protocols and standards. In addition to that, there is significant ambiguity regarding data ownership regulation.

Integration: multiple devices & protocols

Integration of multiple devices also causes hindrance in the implementation of IoT in the healthcare sector. The reason for this hindrance is that device manufacturers haven't reached a consensus regarding communication protocols and standard.

2) An online pharmacy, internet pharmacy, or mail-order pharmacy is a pharmacy that operates over the Internet and sends orders to customers through mail, shipping companies, or online pharmacy web portal.

Online pharmacies include:

Pharmacy benefits managers – Entities that administrate corporate prescription drug plans.

Legitimate Internet pharmacies in the same country as the person ordering.

Legitimate Internet pharmacies in a different country than the person ordering. This type of pharmacy is usually licensed by its home country and follows those regulations, not those of the international orders.

Illegal or unethical internet pharmacies. The web page for an illegal pharmacy may contain lies about its home country, procedures, or certifications. The "pharmacy" may send outdated (expired shelf life) or counterfeit medications and may not follow standard procedural safeguards. Conventional 'bricks and mortar' pharmacies usually have controlled drug distribution systems from the manufacturer, sufficient validation, and follow good distribution practices. Home delivery of pharmaceuticals can be a desirable convenience, but sometimes it can lead to problems with uncontrolled distribution.

The shipment of drugs through the mail and parcel post is sometimes a concern for temperature-sensitive pharmaceuticals. Uncontrolled shipping conditions can include high and low temperatures outside the listed storage conditions for a drug. For example, the US FDA found the temperature in a mailbox in the sun could reach 136 °F (58 °C) while the ambient air temperature was 101 °F (38 °C).[1]

Shipment by express mail and couriers reduces transit time and often involves delivery to the door, rather than a mailbox. The use of insulated shipping containers also helps control drug temperatures, reducing risks to drug safety and efficacy. International consumers sometimes purchase drugs online from online pharmacies in their own countries or those located in other countries. Some of these pharmacies require prescriptions while others do not. Of those that do not require prescriptions, some ask the customer to fill in a health questionnaire with their order. Many drugs available at legitimate online pharmacies are produced by well-known manufacturers such as Pfizer, Wyeth, Roche, and generic drug makers Cipla and Ranbaxy of India and Teva Pharmaceutical Industries of Israel. However, it remains difficult for a patient to ascertain whether an online pharmacy is legitimate. Medicines obtained from rogue online pharmacies come with no guarantees concerning their identity, history, and source. A study in three cities in the Netherlands found that over 60% of the consumed sildenafil was obtained from illegal sources.[10] Roger Bate from the American Enterprise Institute tested hundreds of prescription drug orders purchased over the Internet and discovered that properly credentialed online pharmacies, ones selling dom

3) a} domE-Governance can be defined as the application of communication and information technology for providing government services, exchange of information, transactions, integration of previously existing services and information portals It makes the whole administrative process convenient, efficient, transparent, fully accountable and responsible. As a fast-growing economy and an emerging world leader, E-Governance is a

must in a country like India, both in Government and corporate sector.Some effective examples of successful implementation of E-Governance to the governmental function include projects like; e-Mitra project(Rajasthan), e-Seva project(Andhra Pradesh), CET(Common Entrance Test)estically and internationally, only sell lawfully-manufactured medicines. The use of e-governance helps make all functions of the business transparent. All Governmental information can be uploaded onto the internet. The citizens access specifically access whichever information they want, whenever they want it, at the click of a mouse, or the touch of a finger. However, for this to work the Government has to ensure that all data as to be made public and uploaded to the Government information forums on the internet. AccountabilityTransparency directly links to accountability. Once the functions of the government are available, we can hold them accountable for their actions. In today's internet's time, we can talk to someone who in another corner for the world and we can send an e-mail in just a few seconds. Technology and the internet have made the money transitions secure, fast and free from much human interference.The process of globalisation is a gift of technology and due to the technology and its benefits, the concept of E-governance is introduced in India. The 'E' in E-governance signifies electronic and E-governance means the governance with Information technology. The increasing demand for transparency in administration, faster information transfer and other demands that can be fulfilled by the E-governance only pushed the government and public sector to chose E-governance. The model of E-governance is highly successful in developed countries like the United Nations and others but in a counter like India, there were some doubts about its success. India is a country with much diversity. It has a different language, culture, and states with different geographical structure. So it was not easy for all to understand the policies of the central government and roaming around the state and central government's offices to get some of their work done. The idea of E-governance introduced efficiency, Promptness, transparency and better citizen friendly interface. A few departments have implemented E-Governance with perfection and they are offering the best services to the citizen of the country. The railway is one of those departments who has applied E-Governance to offer better citizen friendly interface. Now it has become easy for the countrymen to book the tickets for their train journey without visiting the railway station in their city or village. In case of an emergency, the passengers can get help from the government with a tweet only. Another benefit of E-Governance is very much visible on E-Tender. Earlier it was said that there is always some scam or bribe was associated with the government tender systems but now with E-Tenders, it has almost vanished. Almost all the ministries and the department of state and central government have their websites. From these websites, you can get the desired information. Both states and the central government are working to implement technology in government work. The pace of some states is good and some are working steadily and slowly. India has a good position in Asia for the implementation of ICT (Information Communication Technology).

B} There are many challenges in implementing E-governance model in India as well as at global scale. The actual challenge is how to develop and withstand successful e-governance projects and deliver state of the art e-services to inhabitants. Unfortunately, it is not as easy to develop e-governance website in service delivery mechanism. Efficacious e-governance

initiatives can never be taken in hurriedness. With reference to India, e-Governance should enable seamless access to information and seamless flow of information across the state and central government. With reference to India, e-Governance should enable seamless access to information and seamless flow of information across the state and central government. The International Data Corporation (IDC) forecasts that Authentication and Authorization industry, two security components are poised together to grow 28 percent annually to reach more than $7 billion by 2004. This steady growth has heightened security awareness among organizations struggling to mitigate risk while providing anytime, anyplace access to employees, customers, and partners. Security awareness is at an all time high as companies become increasingly Web-centric while breaches in security become mainstream news topics. The computer Security Institute's annual security survey revealed that 90 percent of the respondents in large corporations and government agencies detected security breaches within the last 12 months. Although information security has always had an important role as technology has advanced, it has become one of the hottest topics in the recent past. The Internet's open design and the explosive usage along with rapid adoption of internetworking systems became the prime factor for the tremendous explosion in demand for security services. As the number of potential targets grows, the sophistication of security threats is increasing. Traditional security products such as virus scanners and firewalls do not provide adequate protection against unknown threats and the thousands of mutations and variations of Spyware and viruses available to hackers on the Internet. With the Internet being used in so many ways, the security control of new applications and technologies requires an entirely new paradigm. Security, in this environment of constantly evolving threats, can only come from having complete control of the Internet connection including the ability to specify which applications, known and unknown, can be trusted to use the Internet. Security is neither a software application that can be bought off the shelf and deployed to make a network secure nor a piece of hardware that can guard a network against attacks. A good secured system always ensures the following five basic tenets of security. They are Authentication To address the need to provide trusted access to critical applications, enterprises require solutions that provide authentication and authorization capabilities. Authentication is the process of validating the true identity of another party. Secure systems should incorporate some form of authentication in order to validate the user who is requesting interaction with the system. Organizations need to be able to conclusively verify the identity of individuals and entities before providing the authority and access privileges that allow them to access confidential information or conduct transactions electronically. If users are not properly identified, and if that identification is not verified through authentication, an organization has no assurance that access to resources and services is properly controlled.