An exhaustive survey on security and privacy issues in Healthcare 4.0

The healthcare industry has revolutionized from 1.0 to 4.0 where Healthcare 1.0 was more doctor centric and Healthcare 2.0 replaced manual records with electronic healthcare records (EHRs). Healthcare 3.0 was patient-centric and Healthcare 4.0 uses cloud computing (CC), fog computing (FC), Internet of things (IoT), and telehealthcare technologies to share data between various stakeholders.

Later on, an HER system came, which was used to store the patient records electronically in the database repository, which can be accessed from anywhere using the Internet. However, in today's era, maintaining the patient data privacy is utmost essential to preserve the integrity of the stored data. Healthcare 4.0 keeps the patient's record in the centralized HER system to monitor the patients' health records and delivers the uninterrupted services to them in real-time. Patients' health can be monitored through *wearable devices* WDs and implantable medical devices (MDs). WDs are equipped with various healthcare sensors to measure blood pressure, heart rate, temperature, and glucose level of the patients remotely and store them into the centralized EHR called telehealthcare. It helps to understand the patients' behavior for better or improved care of the patient remotely. IoT with telehealthcare can be used to cooperate and coordinate the disease management. Healthcare IoT has a significant impact on the progress of the healthcare industries.

Patients are more worried about their health-related data privacy and they feel quite insecure about the stealing of personal information by third-party cloud service providers. To ensure the data privacy, researchers across the world have suggested the use of an access control mechanism and for security, suggested the encryption standards. Moreover, the healthcare industries have defined some policies and regulations to access healthcare data are — health insurance and portability and accountability act (HIPAA) and health information technology for economic and clinical health act (HITECH). These standards are to improve the nations healthcare system and mandate it for all healthcare organizations to secure health information.

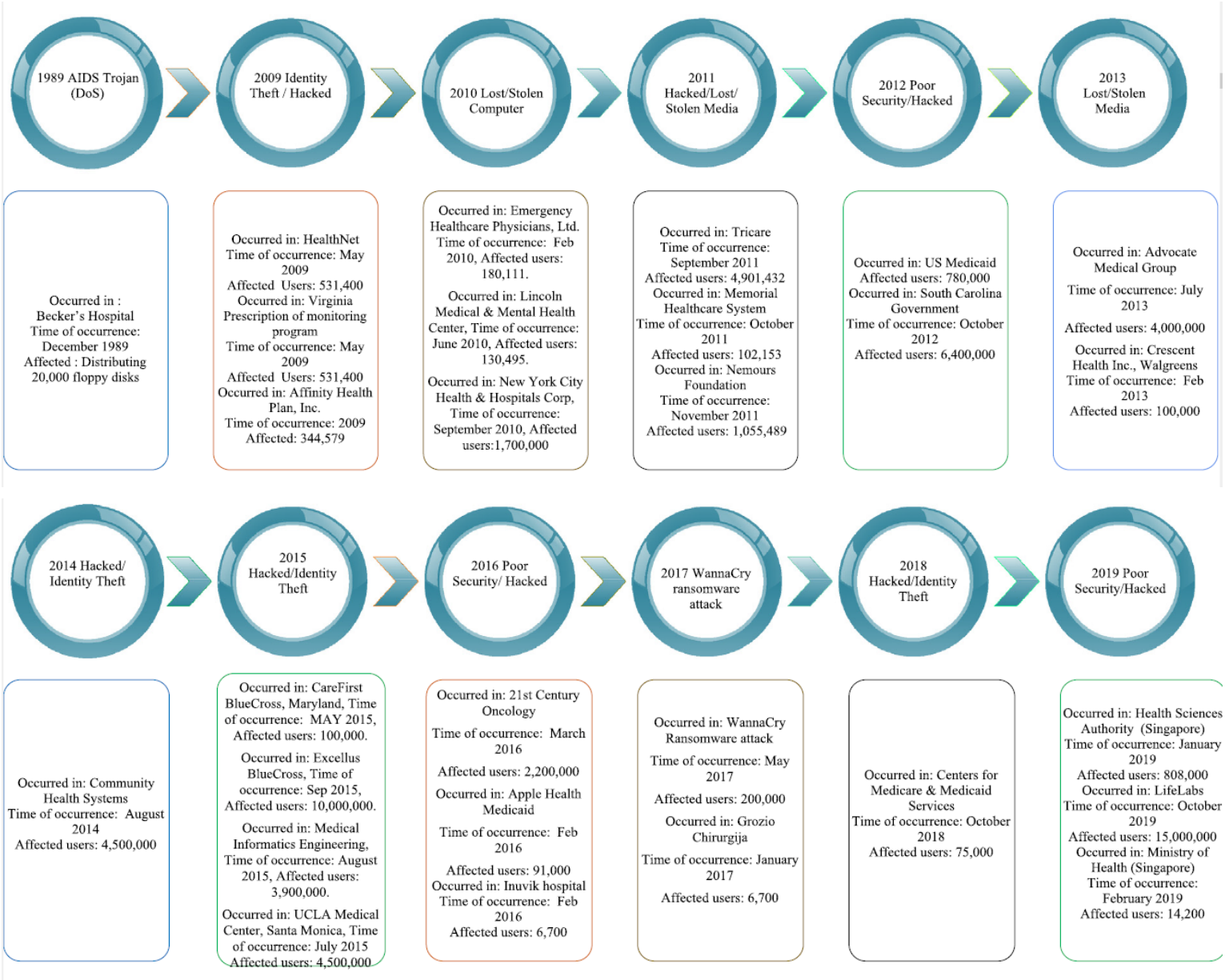

Fig 1. Timeline of security on healthcare data

Security

Security procedures are used to control the access of patient's data to defend it from unauthorized users. It can be achieved with operational controls within a covered-entity. Many countries used personal health information (PHI), which is stored and transmitted through digital systems.

Privacy

In health information, privacy is described as to keep an individual's healthcare information protected from unauthorized access. This can be accomplished with the enforcement of policies and regulations. Privacy means only authorized users can access the health information of the patient and in which situation patient data might be accessed, utilized, and disclosed to a third-party. For example, the HIPAA act ensures the privacy of health data related to the patients.

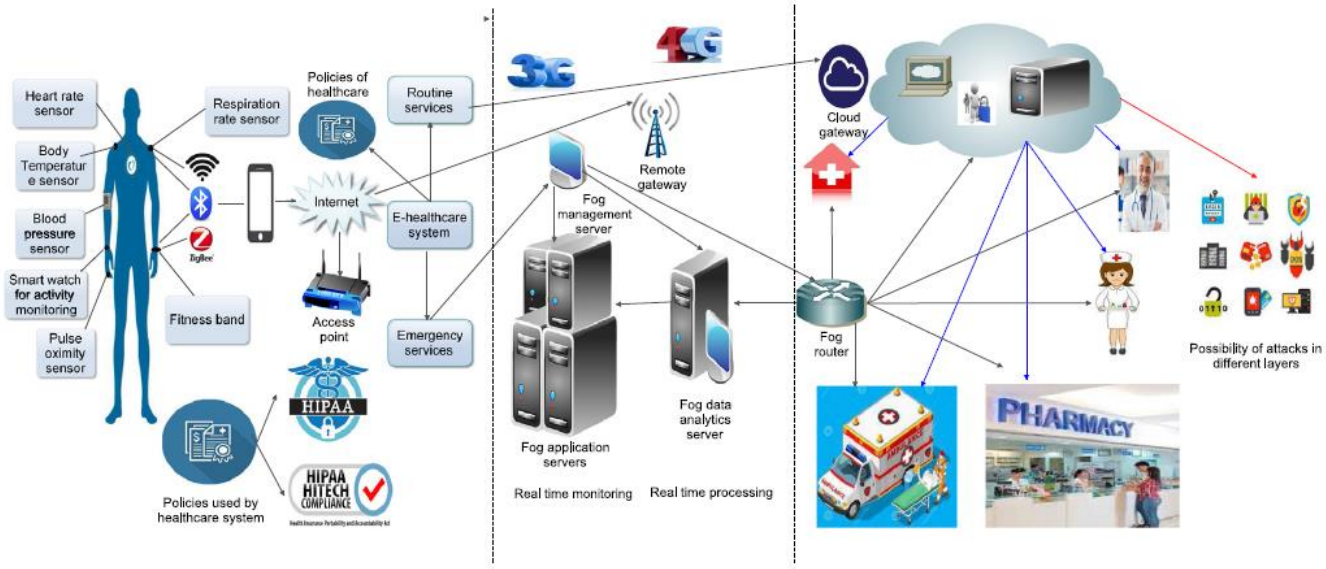

Fig 2. Basic architecture of Healthcare 4.0

Architecture and its components

Basic architecture

There are three-layer e-Health architecture of caregivers and patients where the three layers are: front end, communication layer, and back end, as shown in Fig. 2. The detailed description of each layer is as follows.

Front end: A broad set of IoT-based healthcare devices like sensors, WDs, and MDs are there to monitoring the real-time health status of the patients. This status is verified and stored in the health cloud for further processing. Fig. 2 depicts the complete layout of the e-Health system, where the first layer consists of physical sensors and wearables, which gathers real-time health data from the patients. These sensors transfer the health data to MD using the communication protocols mentioned above and further connects to the Internet to store the data into the cloud storage. Moreover, MDs can have both physical and virtual sensors. A physical sensor monitors the patients health and track their wellness in real-time whereas, virtual sensors gathers the health data from remote diagnostics for remote consultation, remote monitoring, and PHR.

Communication layer: It handles the data that gathered from the front end devices and sends it to the remote gateway through the Internet. Routine services are forwarded through cloud gateway and emergency services are through fog gateway for further analysis. This layer comprises of high-performance low-power FC nodes, which is connected with various wearables

or sensors to process the data accurately. FC solves the issues of network latency and data security of healthcare data. The cloud server analyzes the patient's real-time information and processes it over the broad geographical area, which is quite time-consuming. This issue can be solved using FC for emergency services. In this layer, fog nodes perform aggregation, filtering, compressing, and formatting of gathered health data. To secure this data, authentication, access control, and encryption mechanisms are used by the researchers.

Back end: It consists of a high-computing data center which provides centralized control of the patient, which permits complex and long-term analysis of behavior, and the relationship of patients data. Moreover, it consists of a cloud server that takes decisions dynamically. It is used for data aggregation and provides additional storage to store the medical records of the patient. The doctor, patients can access these records and the pharmacy department (summarization or billing purposes) to get insights. Patients can show their historical and current health records/bills using a web interface or mobile application. The data collected from various sources is integrated into the EHRs, eprescription websites, and web sources. So, doctors and patients can access the information anytime and anywhere as and when they require it. It provides a pushing service to get a notification when any patient upload or receive the health data. In each layer, as discussed above, more than one technology is used to improve the care of the patient. Patient health data are shared over the Internet, which is an open channel and has the possibility of attacks such as DDoS, privileged insider, replay, MIM, impersonation attack. These attacks can be tackled with the usage of security solutions and classical cryptographic techniques.

Fig. 3 Research challenge in Healthcare 4.0

Open issues and challenges

The medical records are transforming into digital records (stored in EHR), which is accessible online through the cloud server. Attackers can easily breach the cloud server security and get unauthorized access to the patient's medical data. This section highlights the various security and privacy challenges in Healthcare 4.0 as shown in Fig. 3.

• *Ethical challenges*: Some ethical challenges like confidentiality, data privacy, data access control, profit-orientation of patients information, possession, and administration are the key elements that obstruct the exchange of data between the patient and HSP. Thus, access to the complete image of the patient data at the time of care becomes a challenge.

• *User authentication*: Authorized users are allowed to access patients' records from EHR. But, an attacker can steal the identity of the user to check the patient's information. But, it is quite difficult and challenging to identify unauthorized access.

• *Confidentiality and Integrity*: Confidentiality hides the critical information from unauthorized users, whereas, integrity ensures data accuracy. Any adversary can modify the stored information

that leads to data inaccuracy. Preventing the data from various security and modification attacks is a very challenging issue.

• *Data Ownership*: Data ownership is ‘‘who owns and access the data’’. Attackers can modify the ownership details to make their ownership invalid. So, preventing the ownership data from unauthorized access is of utmost importance to make the system safe and secure.

• *Data Protection Policies*: The security and strict administration are required for data involved in health diagnosis to prevent it from loss or theft. A secure EHR system needs to be developed with different security levels, which is quite a challenging issue.

• *Misuse of Health Record*: Few websites offer an online EHR system with free limited storage space and are not more concerned about data privacy. They might sell the information or data to another company or advertising agency. Maintaining the security and privacy of health data in a multi-specialty environment is a very challenging issue.

TASK 1

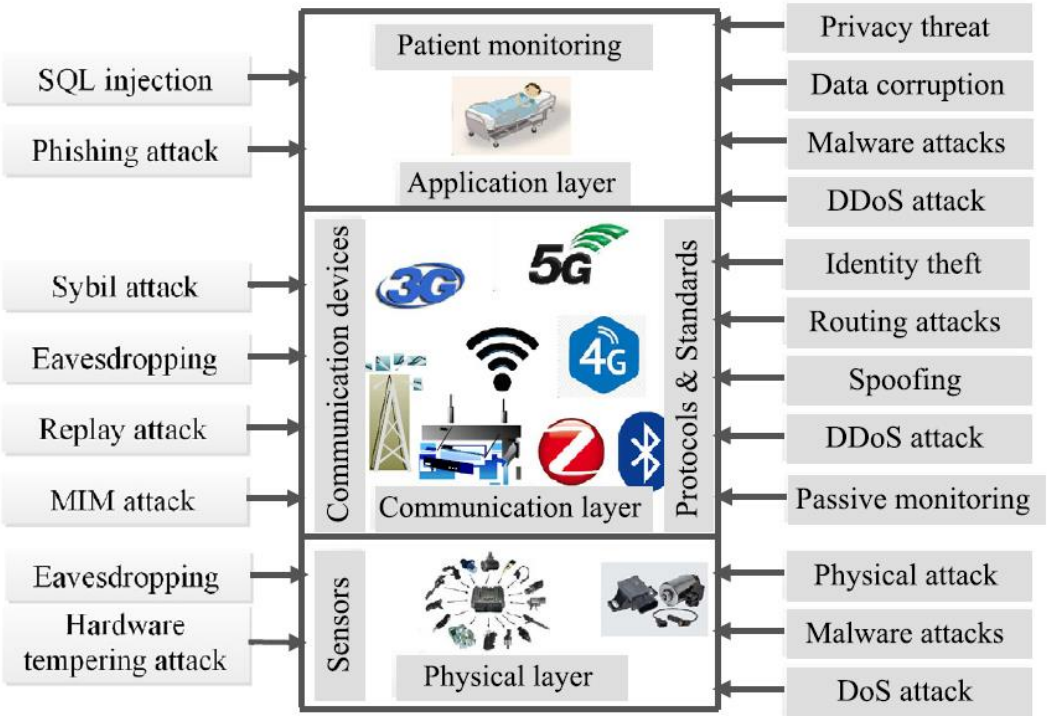

Fig. 4. Possible attacks on different layer.

Berikanlah contoh serangan DDos attack yang pernah terjadu dalam *physical layer, communication layer, dan application layer* baik yang terjadi di Indonesia ataupun luar negeri.

TASK 2

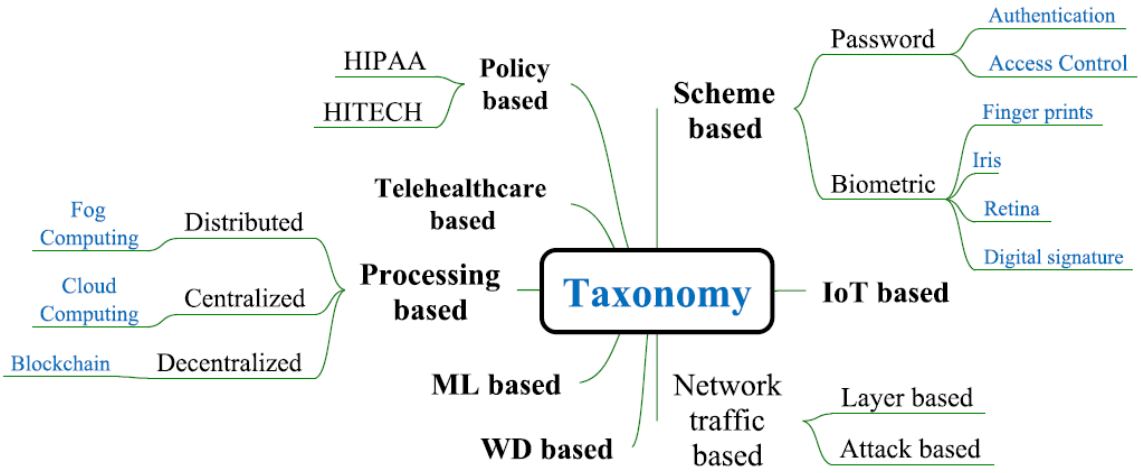

Fig. 5 Solution taxonomy of security and privacy in Healthcare 4.0

Berikanlah Penjelasan beserta contoh dalam menjaga sekuritas dan privasi data dalam pelayanan kesehatan sesuai Taxonomy *policy based (*HIPAA and HITECT) dan *Scheme based (password and Biometric).* Sumber pencarian dapat dalam berbagai jurnal, salah satunya jurnal dengan judul pada modul ini.