Comparative Analysis of Threat Modeling Methods for Cloud Computing towards Healthcare Security Practice

Prosper K. Yeng[1]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway

Stephen D. Wulthusen[2]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway
School of Mathematics
and Information Security
Royal Holloway,
University of London
Egham, United Kingdom

Bian Yang[3]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway

***Abstract*—Healthcare organizations consist of unique activities including collaborating on patients care and emergency care. The sector also accumulates high sensitive multifaceted patients' data such as text reports, radiology images and pathological slides. The large volume of the data is often stored as Electronic Health Records (EHR) which must be frequently updated while ensuring higher percentage up-time for constant availability of patients' records. Healthcare as a critical infrastructure also needs highly skilled IT personnel, Information and Communication Technology (ICT) and infrastructure with regular maintenance culture. Fortunately, cloud computing can provide these necessary services at a lower cost. But with all thees enormous benefits of cloud computing, it is characterized with various information security issues which is not enticing to healthcare. Amid many threat modelling methods, which of them is suitable for identifying cloud related threats towards the adoption of cloud computing for healthcare? This paper compared threat modelling methods to determine their suitability for identifying and managing healthcare related threats in cloud computing. Threat modelling in pervasive computing (TMP) was identified to be suitable and can be combined with Attack Tree (AT), Attack Graph (AG) and Practical Threat Analysis (PTA) or STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege). Also Attack Tree (AT) could be complemented with TMP, AG and STRIDE or PTA. Healthcare IT security professionals can hence rely on these methods in their security practices, to identify cloud related threats for healthcare. Essentially, privacy related threat modeling methods such as LINDDUN framework, need to be included in these synergy of cloud related threat modelling methods towards enhancing security and privacy for healthcare needs.**

***Keywords*—Cloud computing; healthcare; threat modelling; security practice; data privacy**

I. Introduction

Flexibilities of cloud computing has provided huge benefit to variety of users. So, individuals, governmental and non-governmental organizations, SMEs and other companies are adopting cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Adopting cloud computing can be very useful for healthcare organizations. It can enable healthcare organizations to focus on their core business of therapeutic services while maximizing the various benefits such as easy collaboration and data sharing, mobility and cost reduction on ICT services [1]. Cloud computing is a kind of distributed system aimed at providing unlimited shared pool computing resources (hardware or software) to registered users [2], [4].The resources can be scaled up or down to meet each clients' need [4]. Cloud Service Providers (CSP) mostly host services such as applications (SaaS), application development platforms and tools (PaaS) or servers, storage and other virtualized computing resources (IaaS) and makes them available to their clients on the internet. Some of these CSP include Microsoft Azure Services (MAS), Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM, NetSuite and Salesforce [2].

Users who do not have the capacity to acquire and own such systems, can basically adopt to these cloud services as tenants to the providers, at a much lower cost [5]. Institutions which require temporal resources such as storage, processing and development platforms can also leverage on the capabilities of cloud computing. In addition to the lower costs, the tenants of the cloud service companies could benefit from scalability, business continuity, collaboration efficiency, flexibility and strategic values [5], [6]. Based on perceived demand for cloud-based systems, IBM and Active Health Management developed “Collaborative Care Solution” which was implemented in 2010 to support medical staff in accessing healthcare data from different sources [1]. Additionally, the General Electric (GE) also came up with “centricity practice” cloud-based healthcare system [7]. The system was patient centered which enables self-service of patients such that the patient could be able to communicate with their healthcare providers at remote locations but in a secured manner. Similarly, Dell's cloud based solution focused on EHR for small and medium scale healthcare organizations [8]. Additionally, the National Health Service (NHS) in the UK proposed cloud-based solutions for financial relieves. In fact, the need for cloud-based systems cannot be over emphasized but security and privacy hurdles need to be clarified. This study therefore compared threat modeling for cloud computing to assess their suitability for assessing healthcare related threats in cloud computing towards countermeasures. The remaining of the paper consists of the Scope, Research Problem and Contribution. This is followed by the background section which describes security challenges in cloud computing for healthcare, Overview of Cloud Computing, features and Models of cloud Computing, Healthcare related information security threats, threat modelling methods and their related characteristics. The method used in the review, and the findings were provided under the method and findings sections respectively. These findings were subsequently discussed and concluded.

II. Scope, Research Problem and Contribution

Different type of threat modeling methods have been analyzed in regards to their suitability for threat modeling cloud computing environment. But with the need for healthcare to adopt to extra security measures for protecting sensitive data while making it available in a timely way, dedicated threat modeling methods are required.

Therefore, this study reviewed threat modelling methods for cloud computing towards healthcare security practice. To enable healthcare sector to successfully adopt cloud computing, some key issues relating to security, need to be addressed. For instance, what threat modelling methods can be efficiently used by healthcare IT professionals to determine comprehensive threats in cloud computing towards mitigation? How can healthcare staffs' security practice be effectively analysed in the context of big data in cloud computing towards enhancing security?

Though the above questions have not been addressed by existing studies, there have instead been varying opinions regarding effective threat modelling methods for cloud computing [6], [14], [26]–[29]. Additionally, threat modeling methods are being used in their isolated ways in threat modeling healthcare systems. Example, Abomhara et al adopted STRIDE-Based threat modeling method for telehealth systems [56]. Similarly, threat modeling methods were individually used for threat modelling mobile health systems [57], electronic health records system [58] and home care system in the cloud [59]. However, the further question is whether the isolation use of these threat models are effective enough to cover the relevant threats of cloud computing needs for healthcare. This study therefore answered the above research questions, having compared cloud related threat modelling methods and assessed their advantages and disadvantages with respect to threat modelling characteristics for cloud computing and challenges in healthcare.

III. Background

A. Security Challenges in Cloud Computing for Healthcare

According to Shostack et al., cloud computing security challenges can originate from various sources [10]. Using the attacker grouping approach, threats can emanate from both CSP and tenants' sides. The CSP related threats could include insiders who are staffs of the CSP thrust boundary. These insiders may intentionally or accidentally attack tenants or become victim of an attack. Security issues can also originate from all the tenants and other users of the cloud system. Tenants malicious behavior can result in blacklisting effect [9], [10]. Tenants with certain user privileges (such as IaaS and PaaS) could execute malicious codes and the consequences can affect co-tenants and CSP. Additionally, the CSP could be directly targeted by some tenants. Further to this, CSP can face compliance issues. For instance, for CSP to host sensitive applications such as health related or Payment Card Industry (PCI) applications, it is suggested that the CSP must comply with these organizations' requirements. Tenants may also face litigation related issues. For instance, if a tenant requires to know some information about their data which has been held in cloud computing systems for some purposes, they might not be able to get precisely what they want. Data stored on private cloud is more legally protected than data with third party CSP. Forensic response can also be an issue for the tenants similarly to legal related issues. Another source of issue in cloud computing is the usage of mobile devices much like other computing devices [10], [11], [66]. Device loss and the possibility for an adversary to access resources illegitimately is deemed to be a major concern.

According to Cloud Security Alliance (CSA) [11], the security guidance for key areas in cloud computing include data lose or leakage, account or service hijacking, insecure interface, denial of service [12] and malicious insider. Other areas of cloud computing which require attention are data breaches, abuse of cloud services [13], [14], insufficient due diligence and insecure VM migration [14], [15]. Cloud computing is also characterized with various vulnerabilities relating to both technological and human aspects. Some of the common vulnerabilities in cloud computing are session riding, virtual machine escape [14], obsolete cryptography, unauthorized access to management interface [7], internet protocol and data recovery. Additionally, metering and billing Systems and Vendor lock-in are some of the security concerns in cloud computing [14]. In vendor lock-in, for instance, a healthcare organisation could move its IT operations to a cloud provider and subsequently realised it can cannot easily move in the future to a different provider without substantial costs, legal constraints, or technical incompatibilities [62], [66].

In a dynamic and distributed network environment characterized with many users, resources and omnipresent electronic devices, there is a need to adopt to appropriate threat modelling methods to adequately identify related threats and vulnerabilities for efficient measures. The aim of this study was therefore to present the state-of-the-art threat modelling methods that can be used to effectively analyse and identify information security related threats in cloud computing. In this section, the overview of cloud computing and the research problem was presented. This was followed by a presentation of threat modelling methods in Section 2 as the state-of-the-arts. The Section 3 presented the the methods used. In Section 4, the findings and gap analysis of the cloud related methods which were found in the state-of-the-art, were presented and compared. A discussion and conclusion on the state-of-the-art were presented in Section 5.

B. Overview of Cloud Computing

Cloud Computing arose from parallel computing, through grid and utility computing [2], [3], [16]. Parallel computing involves the simultaneous use of multiple homogeneous processing elements in solving a scientific problem. The problems are usually broken down into smaller tasks which are then solved at the same time with multiple processors [2], [17], [18]. The purpose is to safe time, money and to overcome complex tasks while efficiently utilizing the computing power. Application areas include military, energy exploration, data bases and data mining, real time simulation of systems, advanced graphics, augmented reality and virtual reality [2], [17], [18].

Grid computing is a form of parallel computing which uses a network of computers with many CPU cores spread across multiple locations to execute a task instead of the usage of many CPU cores on a single machine [2], [19]. Grid computing is a decentralized service, involving multiple computers with heterogeneous operating systems at different physical locations [2], [19]. Utility computing aimed towards providing resources to clients in a scalable fashion based on the clients' demands and this translates into corresponding scalable pricing [2], [20]. Basically, utility computing maximizes resource usage while minimizing cost of service provision [2], [20]. SaaS is mostly suitable for SMEs to use advanced technologies at lower costs [2], [20]. SaaS involve delivering application software over the internet at flexible packaged payments for license and maintenance fees [2]. Within cloud computing, edge computing is a distributed paradigm in which data storage and computing power is moved closer to the devices or data sources [60] while fog computing is a form of cashing which enables devices to access and process data within the local network when internet is unstable [61].

C. Features and Models of Cloud Computing

The features of cloud computing can be categorized into physical and operational or functional features. The physical features include client side, internet, distributed servers and data-centers [2], while the operational or functional features include on-demand self-service, resource pooling, elasticity, measured service and ubiquitous network access [21]–[23].

The clients include computing resources, such as hardware or software, which are dependent on cloud computing and are being used by the end users for service delivery [2], [22]. The clients can be specifically designed for the cloud and therefore becomes useless without the cloud computing.

The computers may include thin clients, mobile devices and thick clients. The software which are being used by the cloud users are usually hosted in several servers known as the data center [2], [22]. A data center consists of a large group of networked servers, either in a room or building, housing the servers for remote processing and storage or distribution of large amount of data [2]. A server can contain many virtual machines (VM) which the number of VM per server depends on the speed and memory size of the host among others. For resilience such as reliability, availability and fault tolerance, servers can be distributed across geographical locations. The distributed server feature of the cloud computing also helps in scalability [2], [22].

The operational features include elasticity, measured services, ubiquity, resource pooling and on-demand self-service [2], [22]. Elasticity feature defines the property of cloud computing which enables scaling up or down of the unlimited resources to meet the needs of the users. Measured Service is the ability to measure exactly, the cloud services usage per clients despite the shared pooled resources by many clients. Ubiquitous Network Access feature provides access to the cloud computing resource on the network which can be accessed by different type of clients such as mobile phones, laptops and desktops at different location. Resource Pooling enables cloud provider to provide services to the subscribers through a multi-tenant type. Cloud computing resources are assigned and reassigned, following the subscriber needs. On-Demand Self-Service enables a cloud user to use cloud services as needed and without human interference.

Cloud computing models can be categorized into business models and deployment models [2], [22]. The business models include SaaS, IaaS and PaaS while the deployment models include public, private, community and hybrid cloud models. SaaS model enables the provider to provide software services to their clients or subscribers. The clients can rent the software from the providers via internet and the software should be able to react to the clients' interface to appear as if the software belong to him only despite other client are using the same software. PaaS enables users to develop their own applications by renting the development environment and toolkits from the cloud computing providers. The development toolkits are usually accessed from the cloud by the developers through the web browser. Other resources such as operating system, processors, memory and storage of the application development files are provided by the cloud computing provider [2], [24]. CSP also provide the infrastructure as a services (IaaS) to clients and the usage time are quantified per CPU utilization per hour, usage of storage and data transfer rates [25]. There exist other cloud services such as app's stores, online games and electronic books but this study focused on the IaaS, PaaS and SaaS models.

Each of the different deployment models of cloud computing (such as the public, private, community and hybrid) have its related security repercussions. The public cloud computing model is usually patronized by the general public as pay per use or use for free arrangement. Example of such cloud providers include Amazon's AWS, Microsoft Azure and Rackspace Cloud Suite [2], [4]. Private cloud computing model is usually provided by an organization behind its firewall for accesses of members of the organization only. The services of the private cloud computing model are usually restricted from public access and the IT Network administrators of the organization's data center are usually the cloud providers. The community cloud computing model is a kind of public and private model, which is setup for a specific purpose. Essentially, the advantages of cloud computing are transforming the way cloud computing users work. Users can globally access all their programs and documents from any computer via the internet such that the user is no longer tied to a single computing device such as a particular laptop computer to access data and resources. In addition, cloud computing enhances group collaborations, since all group members can flexibly access the shared resource in the cloud from wherever they are located but effective security measures are required [24].

D. Healthcare Related Information Security Threats, Threat Modelling Methods and their Related Characteristics

Threat modeling is the use of methods to help in thinking, identifying and enumerating possible risks and threats [6], [14], [26]–[29]. Threat modelling also helps in the identification of the lack of security controls for mitigating risks [6], [14], [26]–[29].

Various type of threat modelling which were identified in this study include Attack Tree (AT), Attack Graph (AG),Attack Surface (AS), Practical Threat Analysis (PTA) , Threat Model Framework for Personal Network (PN), STRIDE, Threat modeling in pervasive computing paradigm (TMP), [6], [14], [26]–[29], [50] and LINDDUN (Likability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness and Non-Compliance) [30] as defined below:

Attack trees provide a structured way of describing [10] threats and vulnerabilities of a system, with regards to varying attacks and shows the possible attack paths which attackers can follow to be able to compromise the system [26].The attacks are represented against the system in the form of a tree. The goals are placed as root nodes while the leaves nodes represent the different ways of achieving the goals. Attack trees are widely used for security modelling and analysis in the cloud computing. The general steps involves in the attack tree include [26]:

- Specifying the attacker's main goal and this is termed as root node. An Example could be for the attacker to access assets such as data in the cloud.
- Decompose the main goal into sub-goal which is termed as leave nodes: Example include attack repository, get credentials through social engineering; attack certificate or Attack Web portal.
- Continue to divide the sub goals into stepwise subtasks.
- Assign the leave nodes with attribute values.
- The security of the goal can then be computed after all nodes are computed

Attack graph adopts to graphic view of all attack paths including attack point to attack target [27]. Attack graph assesses network configuration and vulnerability information of network by obtaining the entire dependency interactions of the information. Attack surface captures software features that have the tendency to contribute to vulnerabilities. Some of such features includes entry and exit points communication channels, and untrusted data items.

TAM is based on business objectives [14] which involves the business needs and issues that must be met by the system. This is followed with system components. The components include application architecture, user roles, trust level, authentication mechanism and external dependencies. The third level involves generating threats and classifying them into CIA traits. Finally, each threat is assessed based on business need.

PTA process involve identifying assets and their related financial values. The PTA provides tools to enable providers to obtain the value of assets and potential level of damage that can be caused by the adversaries. This is followed with the identification of vulnerabilities , the assessment of risks of threats and specifying the risks mitigation strategies of the system. The identification of vulnerabilities is based on the assessment of the architecture of the system and different type of users.

PN is a user centric network which consists of users' network devices known as personal devices. The network composed of applications, telecommunication, environment and services for the users. The first step in PN framework focused on describing a use case to include everything in the network from the users' perspective. The second step involve gathering network requirements from use case diagrams, network architecture, environments and technologies. In the third stage, data flows are clarified using UML sequence diagrams and the determination of actors and devices involves. Asset identification and determination of all threats were subsequently followed. Vulnerabilities were then identified, and the risks were therefore determined from the threat and vulnerabilities profiled. Finally, the threats and vulnerabilities were rated.

STRIDE is a threat modelling framework which is focused on identifying threats relating to spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privileges [14]. Various sources [10], [31]have indicated that STRIDE framework can be used based on per-element of the cloud system or per-interaction with the cloud system. STRIDE-per-Element involves enumerating various elements of the system and assessing for the specified threats around each element. This approach simplifies the finding and identification of threats which are associated with each element. But STRIDE-per-Interaction identifies threats based on the origin, destination and interaction attributes of elements, which also makes it easier to understand related threats. STRIDE approach generally provides guidelines as what threat to look for and where they can be found. STRIDE seeks to identify and mitigate threats and vulnerabilities through the reduction of the cost of entire development process. The STRIDE based modelling follows five systematic steps beginning from, classifying assets, obtaining the overview of the system by creating DFD. Threats are then modeled and identified. The identified issues are addressed and the threats are eventually ranked by using Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD).

With Threat modeling in TMP, all cloud computing users' roles are identified in relation to their service usage and authentication mechanism in the first step. The second stage involve identifying security domains to understand how users interact with applications within the domain. Trust levels were subsequently identified so that users can access resources based on their level of trust level. Vulnerability identification is done in the next level so that known vulnerabilities can be mitigated while unknown vulnerabilities are managed in a manner that would protect the system. Risk evaluation are performed in the next stage to provide knowledge for appropriate risk management strategies.

In the area of privacy, the LINDDUN (Likability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness and Non-Compliance) privacy threat modeling framework has recently gained attention in the privacy community [30]. LINDDUN provides systematic support to elicit and mitigate privacy threats. The strength of LINDDUN is its systematic approach in guiding the analyst through the privacy assessment exercise effort, combined with its extensive privacy knowledge base.

Within the healthcare domain, it is critically important to correctly identify patients and correctly map them to their health related records [55]. This compels healthcare organizations to collect and store detailed amount of personal identifiable healthcare data from each patient, making it rich for committing identity theft [55]. Therefore, in the development of health information systems, security practice relating to threat modeling should adequately be adopted to rigorously protect the systems. Some of the dimensions of threat areas in healthcare have been identified to include malicious users, misuse of information system resource, communication interference, damages, failures, errors and threats relating to theft. Others include repudiation and attribution, misuse of system resources, legal and regulatory requirements as shown in Table I. These related threats are not unique to health information systems, however, threat impact of the aforementioned can have life-threatening impact on the vulnerable patients [55].

IT staff in healthcare who have the responsibility of managing the development of healthcare systems will need to comply with various security practices [54] including threat modeling to identify attackers, resources or assets can be compromised and their mitigation strategy.

In summary, threat modelling methods for cloud computing in healthcare should have the outlined abilities [10], [14], [32] as shown in Fig. 1. The characteristics includes:

- Identifying and classifying assets: IT assets within healthcare includes but not limited to data, software or hardware which are being used by the healthcare providers. All these assets need to be identified and categorize for efficient security management. For instance, assets can be classified based on different values, damage costs and trust levels to enable prioritization for countermeasures.
- Identifying users and threat agents: For each user domain, different users with different access controls have different trust. Example, different healthcare staffs such as administrators, all authorized users and unregistered users have different trust levels [31]. Additionally, a threat can adversely act on assets. Threat agents includes unauthorized entities, system administrators and other authorized users. Natural events including flood, earthquake, and fire can also be a threat agent. All these need to be identified for effective security management [35].
- Establishing trust level and User's Role: Establishing thrust levels and linking it to established healthcare professionals' roles with authentication, authorization and access control mechanisms, enhances the confidentiality, integrity and availability of the assets [36].
- Identifying Security Domain: Different user domains have different security levels with their respective different kind of information types. Therefore, it is important to separate domains for security reasons and isolate risks based on the identified security domains [37].
- Identifying Threats and Vulnerabilities: In adopting cloud computing, healthcare organizations are inadvertently outsourcing their computational resources on virtual domains. The huge and sensitive amount of data can be damaged by threats from different resources including employees' activities and malicious attacks. So threat and vulnerabilities to the data need to be assessed [38].
- Ranking and measuring vulnerabilities: This enables organizations to identify various weaknesses around their information systems and provides them with the knowledge to prioritized the implementation of countermeasures [39], [40]. The Common Vulnerability Scoring System (CVSS) [41] is one of the methods for rating IT vulnerabilities. The CVSS has base metric, temporal metric and environment metric for evaluating security vulnerabilities. Base metric assesses the basic attribute of vulnerabilities. The environment metric evaluates vulnerability metrics that are associated with the environment and temporal metric considers dynamic aspect of the vulnerabilities.
- Ranking and measuring threats: Ranking and measuring threats is used to assess the risk posed by the identified threats having taken various factors into consideration. The first step is to consider the risk level which is posed by each threat. So, Microsoft Threat Modeling introduces Damage potential, Reproducibility, Exploitability, Affected users and Discoverability (DREAD) as a type of threat ranking and measuring method as follows: The equation that is used to compute a risk value has been shown as follows [32].

  $$Riskvalue = (D + R + E + A + D)/5 \qquad (1)$$

  The risk value is between the range of 0 and 10, so that the risk increases with higher risk values. Similarly, the Open Web Application Security Project (OWASP) measures risks based on the likelihood of the threat and its related impact as follows:

  $$Risk = Likelihood * Impact \qquad (2)$$

  Applying Common Vulnerability Scoring System to a business process cannot fully deliver optimal security measure in dynamic environments [33]. VRank and hybrid ranking have been developed to satisfy business requirements. The VRank [34] as a dynamic framework is able to integrate existing vulnerability databases with the specific detail context of business process. Accordingly, the VRank provides more specific vulnerability assessment for SOA. The hybrid ranking model proposes a combination of CVSS rating and numerical estimation of vulnerability that influence the global network [33]. By developing dynamic environments estimating vulnerability in an influential level and aggregating other rating models with high-level rating technics provides a hybrid model to precise measurement of vulnerabilities more economic and efficient.

TABLE I. POSSIBLE THREATS TO HEALTHCARE [55]

Related Threats	**Description and Possible harm**	**Instance**
Threats resulting from errors	These include operation errors, maintenance errors, user error and accidental miss-configurations or miss-routing. Operation errors can result in intentional disclosures of confidential information. Maintenance errors such as miss-configurations of software can be committed by staff members or third party employees who are responsible in maintaining the systems. If the miss-configuration has to do with authentication and authorization, serious consequences can be uncured. Legitimate accesses for therapeutic purposes can be denied and this can lead to further worsening of health conditions and lost of lives. Conversely, miss-configuration of authorization and authentication mechanisms can enable broad access to large and wide number of unauthorized users and this can lead to huge compromise of privacy and security over the cloud computing.	According to [68], [69], errors such as misconfiguration due to human error in cloud infrastructures has increased by 424%. Example, in February 2019, the University of Washington Medicine exposed the information of approximately one million patients due to accidental removal of website server protections [68], [69].
Communication Interference	This includes both the interception and infiltration of the communication of healthcare information systems. Communication infiltration occurs when the adversary tempers with the normal flow of communication and this can lead to denial of service. Additionally, if the message in the communication channel is not protected during transmission, the confidentiality of patients records that are involved, will be compromised if the message is intercepted. Since access to healthcare records for therapeutic purposes is time sensitive, denial of service can also have life-threatening consequences.	In a recent ransomware attack at Duesseldorf University Clinic in Germany, the medical records of a patient were not timely available in an emergency case and the patient loss her life as a result [63].
Unauthorised users	These include insider and outsider masquerades and other unauthorised users who illegally accesses healthcare information and breaches confidentiality, integrity and availability of the system [43]–[45], [52]. . Cloud computing tend to host a number of tenants who are their internal users. Not all internal users of the cloud are necessarily, the internal users of the healthcare facility and their security indiscipline can tend to negatively affect healthcare. Clearly, the healthcare faces broader scope of threats from unauthorised users. Example include all the internal users of the cloud computing system and the exclusive users of the healthcare organization such as a patient who overtakes an unattended workstation in a physician office and accessing the data. Also, when a healthcare professional is to takeover a shift from a colleague, due to inconveniences, the first user may fail to logout in order for the colleague who is taking over to continue work without going through the pain of logging in.	Insider masquerade include an instance in the UK, where DR. Harold Shipman tried hiding a number of records of his patient who is a notorious murder [45].
Threats relating to damage	This includes willful damages by insiders, outsiders, terrorists, and the introduction of damaging and disruptive software or malicious codes. Example include threat of information security systems by co-tenants, disgruntled staff, patients or relatives which leads to availability problem of the CIA.	Terrorists for instance can target large installations of healthcare systems of which the impact could be huge. Example include data breaches in Helse Sør-Øst RHF (Health South-East) of Norway of which the focused was on patient records and the health service's relationship with Norway's armed forces [65]
Threats of failures	Failures include connection failures, technical failures of hosts, storage systems, and network infrastructure, network software failure, application software failure. Others include environmental support failures (eg power failure, failure from natural disasters and man made disasters), and staff failures or shortage. Such impact could compromise with the CIA of the information system in various ways	For example, it was suspected that, the failure to update legacy windows XP resulted in a compromise of about 3million patients records [65]
Theft	Threat of theft include insiders and outsiders who can steal equipment or data in order to sell or disclose to others. Compromising confidentiality and integrity	A laptop of a vendor of Health Share was stolen. The laptop contained 654,000 patients records consisting of names, contact details, date of birth and medical ID numbers of patients [64].
Repudiation and attribution	When there are issues, the ability to determine in time whether the issue is originating from the cloud provider, or the hospital end in a timely manner is a concern.	Example includes a medical record alteration by a cloud maintenance officer who uses the account of a healthcare staff. As the logs of accesses are controlled by the cloud provider, their timely access by the hospital could be a problem. Also, how to ensure non-repudiation even if the logs were provided to the hospital is problematic.
Misuse of system resources	This include scenarios where users tend to use information systems and services for personal purposes. Such activities include misuse of internet and computing resources which an tend to threaten the availability of these systems for healthcare functions.	Example, healthcare workers may tend to be downloading or watching large files of videos on the hospital's network, slowing down the network access for healthcare purposes [52].
Legal and regulatory requirement	Regulatory requirement such as GDPR or HIPAA need to be considered. Example, if sensitive data are to be processed outside EU under the GDPR, there can be a constrain if some of the servers and data processing are carried out outside EU.	Example, if healthcare data from EU is to be stored in third countries, those countries have to be under Adequacy Decision or adopt to additional safeguards to comply with the GDPR else, the DGPR will be violated [67]–[69].

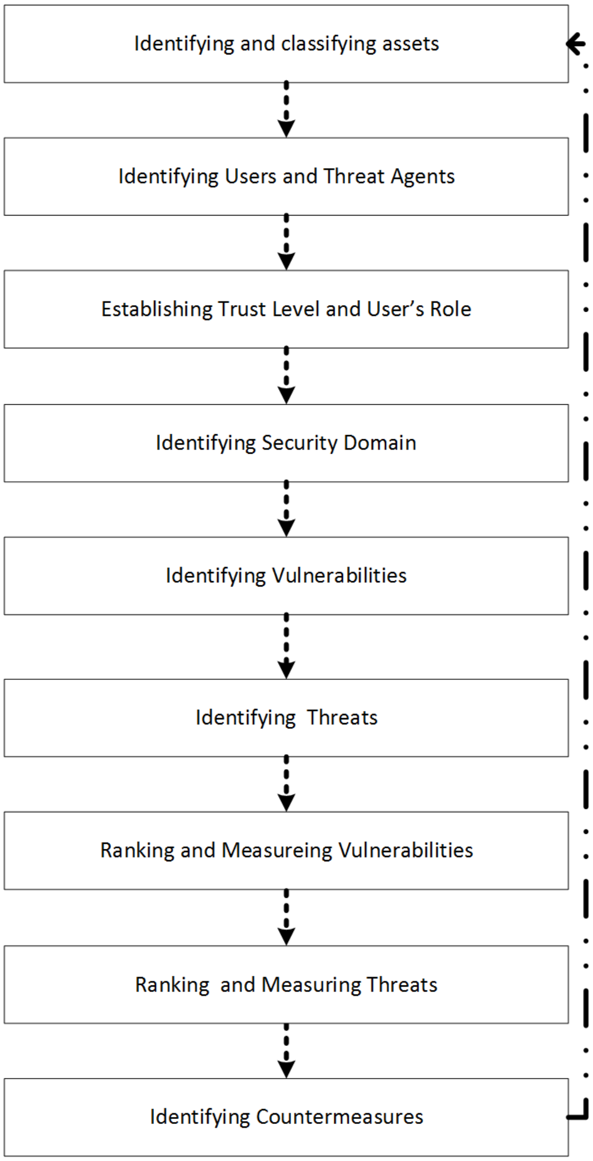
Identifying and classifying assets
Identifying Users and Threat Agents
Establishing Trust Level and User's Role
Identifying Security Domain
Identifying Vulnerabilities
Identifying Threats
Ranking and Measureing Vulnerabilities
Ranking and Measuring Threats
Identifying Countermeasures

Fig. 1. Characteristics of Threat Modelling for Cloud Computing [31], [32]

- Identifying countermeasures: Information security countermeasures include actions, devices, procedures, techniques and other measures which are adopted reducing vulnerabilities towards protecting assets against threats [42]. The appropriate countermeasures are identified based on the measured threats and vulnerabilities. Identifying new assets, vulnerabilities and Threats [31].

Threat modeling and its countermeasure should not be a one-time event but an ongoing process in cloud computing in healthcare. This will enable the identification of new assets and associated threats and vulnerabilities as shown in Fig. 1. Additionally, users of the system ought to be conscious of new vulnerabilities and their countermeasure. Mitigation procedures need to be adopted for the identified new vulnerabilities to keep the system secure against the new threats [31], [32]. Ideally, the threat modeling methods for cloud computing should systematically cover all the outlined characteristics as shown in fig. 1, from identifying and classifying assets, to identifying countermeasures. Furthermore, the process of detecting new assets, threats and vulnerabilities should be a looping process since cloud computing environment is a dynamic system with evolving potential set of new threats and vulnerabilities.

In a related study, some of the threat modelling methods which were assessed include Microsoft threat modeling with STRIDE, TAM, PTA, Personal network threat modeling (PN) and pervasive computing threat modeling. None of the reviewed threat modeling methods was found to be fully suitable for cloud computing systems [14]. But pervasive computing threat modeling had most of the threat modeling traits (as shown in Figure 1) of cloud computing.

Similarly, attack surface, attack trees and attack graphs, were used to undertake threat modeling exercises in cloud computing infrastructures [26], [28]. Additionally, Cheng et al., generated attack graph model [27] of a cloud computing system and subsequently suggested two security evaluation metrics after combining Markov Chain with attack graph. In the study [27], various assumptions relating to cloud computing system were made.

Based on the effective way of how STRIDE framework categorizes threats, [6] Hong et al. identified cloud related threat through literature survey and categorized them with the STRIDE framework [6]. Basically, the various attacks on cloud computing were categorized with OWASPs attack categories. The attacks were further categorized into cloud computing related threats with the STRIDE framework and the cloud components were mapped to the possible threats. The study was used to propose traceability method for identifying cloud related threats. Furthermore, Yahya et al. adopted STRIDE with a three step threat identification features thus characterizing the system, assets and access identification and threat identification [29], to analyse threats in a cloud storage scenario. In this scenario, the adversary's main target was on the software related services such as SaaS cloud resources. Cloud computing related threats were subsequently identified and classified with the STRIDE method [29]. The threats which were identified in the study were mapped to security requirements objectives.

IV. Method

A literature search was conducted in Google scholar, IEEE Explore, ACM Digital Library and Elsevier for cloud related threat modeling methods. Only threat modeling methods which were assessed for cloud computing, were included in the study. The threat modeling methods were then assessed for their suitability towards effective identification and analysis of threats in cloud computing in healthcare context. Additionally, the threat modeling characteristics were also identified from related studies [10], [14], [32] and these were analysed in healthcare scenarios as shown in table II. The identified characteristics were mapped to cloud relating threats in healthcare context which have been identified in table I. This depicted the role of each of the threat modeling characteristics , in healthcare scenarios as shown in Table II. These characteristics were used as benchmark in the comparison of the identified cloud related threat modeling methods in this study as shown in Fig. I and Tables II, III and IV. The findings and gaps are presented under Section IV.

In the review assessment, each of the threat modeling methods was reviewed against the identified cloud computing threat modelling traits as shown in Table II, Table III and Table IV. Each of the methods that supports any of the particular cloud modeling characteristics, was assigned with a value of "Yes" in its cell in Table IV. However, in the review, if a particular threat modeling method does not support any of the outlined cloud computing threat modelling characteristics, then a value of "NO" is assigned to that threat model. Findings of the entire assessment is presented in Table IV.

V. Findings

The suitability of the identified threat modelling for assessing threats and vulnerabilities in cloud computing were compared as shown in Table IV.

The threat modelling methods were compared against threat modelling characteristics of cloud computing as shown in Table IV. On Table IV, 'Yes' means the method supports the threat modelling traits, 'No' means the mettahod does not support the threat modelling characteristics. In summary, TMP supports almost all the provision for all cloud computing threat modelling characteristics except establishing user's role, scanning domain security and ranking and measuring vulnerabilities [14] and followed by AT as shown indicated in Table IV. On the contrarily, TAM methods provide for only identification and classification of assets and ranking and measuring vulnerabilities [14]. Similarly, STRIDE method has provision for assets identification and classification of assets, identify threats and identify vulnerabilities [6].

A. Gap Analysis

The various studies in threat modeling methods which were explored for cloud computing in healthcare, are shown in Table III and Table IV. In following the characteristics of cloud computing models, there are various gaps in the threat modeling methods. For instance, attack trees and graph mostly support in identifying a comprehensive attack related threats to a system, however, there are no systematic methods to determine parameter values for each node, especially in an Attack Tree [26], [27]. Additionally, attack tree and attack graphs methods are deemed challenging task, particularly for large sized networked systems [6], [27], [46]. This is because, the number of possible attacks grow exponentially with the growth rate of the number of hosts [46]. Also, attack tree is still a relatively high-level concept, without details about specific ways for exploiting a resource. Similarly, Attack surface heavily relies on experts' knowledge of the system features and knowledge past attacks on the system, using these features [50], [51].

Furthermore, TAM framework does not have features for assets determination and identification of vulnerabilities [14], [46]. Meanwhile, cloud computing have multiple assets from the side of both cloud provider and tenants. Therefore the lack of identification of asset and vulnerability assessment is deemed to be a major shortfall for threat molding cloud computing environment.

Additional, PTA model has no provision to estimate the cost of vulnerabilities [10], [14]. Cost of vulnerabilities is computed with cost of down time, replacement and systems' downtime. The lack of cost of vulnerability hides knowledge and idea of avoiding different kind of threats. Due to pervasiveness feature of cloud computing all known and unknown vulnerabilities need to be assessed and planned for but there is a lack of vulnerability ranking mechanism in PTA. Although, PTA rank threats, but it does so only on the bases of financial value and not functional, technical, strategic or reputational value. In cloud computing, tenants can be users of multiple domains which require the need to comprehensively rank threats from different factors and levels of security such as user roles but not only financial bases.

Furthermore, there is a lack of update model for new threats and vulnerabilities in PN model [14]. But in cloud computing, it is vital to frequently assess new threats and vulnerabilities since users of cloud computing have access to

TABLE II. CLOUD COMPUTING THREAT MODELING CHARACTERISTICS IN HEALTHCARE SCENARIOS

TM Traits	Healthcare Context	
	Scenario	**Remarks**
Identifying and classifying assets	In EHR scencario, the main assets include the sensitive healthcare records [70]. Others include mobile devices, user credentials, and the network of the EHR system.	These assets face the related threats [70] as shown in Table I.
Identifying Users and Threat agents	The users include the healthcare professionals who accesses the system for therapeutic purposes, the paramedical staff, temporal staff, service providers such as contracted service personnel eg system software and hardware engineers [55]. Threat agents include insider masquerades, hackers, and natural disasters, patients or subjects of care.	For instance, a subject of care can access an unattended workstation system thereby, compromising the CIA of the system [55].
Establishing Trust level and user's role	Low trust level require minimum or optional, to no security protection mechanism [71]. However, if the highest level of trust is compromised, it involves, loss of data resulting in long-term and permanent damage to the hospital, patients, or groups of individuals. Therefore, high trust level needs the incorporation of protection mechanisms designed into the system to be commensurate with the expected risk of exposure [71].	Example, a software engineer who have access to the entire EHR system in production have access to the highest trust level, requiring for appropriate countermeasures [71].
Identifying security domains	Security domains are list of objects with similar security requirements that can be access by objects including healthcare professionals and end devices, known as users [72]	Nurses may be in the same security domain which is different from the security domain of healthcare application developers [72].
Identifying threats	All possible threats as outlined in Table I are then identified.	Instances of related threats are shown in Table I.
Identifying vulnerability	Possible weaknesses that can lead to attacks are identified	These include web application vulnerabilities (such as SQL injections, Cross site scripting [72], [73]), cloud related vulnerabilities (malicious insiders such as cloud maintenance engineers) and vulnerabilities relating to end users and devices.
Ranking and measuring threats	Metrics of the threats are assessed and ranked for prioritization regarding counter measures.	
Ranking and measuring vulnerabilities.	Vulnerabilities are also assessed and prioritised.	
Identifying counter measures	Possible mitigation are kept identified [70].	Possible countermeasures include multi-layer countermeasures, multi-factor authentication, access revocations etc, fail safe default, mechanism, least privileges [70].
Defining new assets, threats or vulnerabilities	Due to updates, addition of resources and system upgrades, new assets, threats and vulnerabilities need to be identified	For instance, if a new module or department such as radiology, is added, the process need to be repeated to determine new assets and threats.

TABLE III. THREAT MODELING METHOD

No.	Threat Modelling Method	Reference
1	Attack Tree (AT)	[26]
2	Attack Graph (AG)	[26], [27]
3	Attack Surface (AS)	[26]
4	Microsoft's threat analysis and modelling (TAM)	[14]
5	Practical Threat Analysis (PTA)	[14]
6	Threat Model Framework for Personal Network (PN)	[14]
7	STRIDE	[6], [14]
8	Threat modelling in pervasive computing (TMP)	[14]
9	LINDDUN	[14]

TABLE IV. COMPARISON OF THREAT MODELLING METHODS FOR CLOUD COMPUTING

TM Traits	Threat modelling methods								
	AT	**AG**	**AS**	**TAM**	**PTA**	**PN**	**STRIDE**	**TMP**	**LINDDUN**
Identifying and classifying assets	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
Identifying Users and Threat agents	No	No	No	No	Yes	No	Yes	No	No
Establishing Trust level and user's role	No	No	No	No	Yes	No	Yes	No	Yes
Identifying security domains	No	No	No	No	No	No	No	Yes	No
Identifying threats	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Identifying vulnerability	Yes	Yes	Yes	No	No	Yes	No	Yes	No
Ranking and measuring threats	Yes	No	No	No	No	Yes	No	Yes	No
Ranking and measuring vulnerabilities	Yes	No	No	Yes	No	Yes	Yes	No	No
Identifying counter measures	Yes	No	No	Yes	No	No	No	Yes	No
Defining new assets threats or vulnerabilities	Yes	No	No	Yes	No	No	No	Yes	No

different services and domain which exposes them to different type of attacks. Also, in TMP, cloud based assets management methods need to be considered instead of the traditional asset management approach in threat modeling because assets and resources in the cloud are dynamic.

STRIDE was also assessed to be limited for its effective application in cloud computing [6], [14]. Cloud computing is dynamic and pervasive, and can not be threat modeled with static frameworks such as STRIDE. Furthermore, defining new threats, identifying vulnerabilities and privacy related issues have not also been considered in STRIDE framework thus limiting its applicability in cloud computing. According to

TABLE V. THE FOLLOWING ABBREVIATIONS ARE USED IN THIS MANUSCRIPT:

AT	Attack Tree
AG	Attack Graph
AS	Attack Surface
CIA	Confidentiality, Integrity and Availability
CSP	Cloud service provider
CVSS	The Common Vulnerability Scoring289System
TAM	Directory of open access journals
TMP	Threat modelling in pervasive computing
PN	Threat Model Framework for Personal Network
PTA	Practical Threat Analysis
STRIDE	spoofing, tampering, repudiation, information disclosure, denial1 of service and elevation of privilege
LINDDUN	Likability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information,Unawareness and Non-Compliance

Shostack et al., STRIDE only gathers high level security requirement and not details of what can go wrong in the system [2], [10]. Though, LINDDUN model fill in the gap on privacy requirement assessment, it's focus is generally narrowed to obtaining privacy requirement by mapping data flow diagrams of the system to its application scenarios and related threats [30], [50].

VI. DISCUSSION

Though cloud computing paradigm is providing crucial services [5], [6], its distributed nature (ubiquity, elasticity, many user types and resources) has made it susceptible to attacks. To enable healthcare sector to be able to adopt to the usage of cloud computing services, there is the need to establish mechanisms towards identifying and mitigating its related threats. Based on this, threat modeling methods for cloud computing were explored for their fitness for healthcare purpose as presented in Table II and Table IV. Threat modeling methods which were found to be commonly used for cloud computing include Attack Tree (AT), Attack Graph (AG) and Attack Surface (AS), S Microsoft's threat analysis and modeling framework (TAM), Practical Threat Analysis (PTA), TRIDE, Threat Model Framework for Personal Network (PN), TMP [6], [14], [26]–[29] and LINDDUN. From the findings as shown in Table IV, none of the existing threat modelling methods in the review could be used to completely assess threats and vulnerabilities to meet all the characteristics of threat modelling methods for cloud computing. A related study which assessed a limited number of threat modelling methods (without assessing AT,AS and AG) also observed similar results [14]. This poses a major deficiency in identifying and mitigating cloud computing related threats for healthcare sector. Table IV clearly depicts that if any of the identified threat modelling methods is used for cloud related threat modelling, some of the threats and vulnerabilities relating to the outlined characteristics in Table IV would not be covered. For instance, AG, AS, TAM, PTA, PN and STRIDE have no provision in their framework to determine new assets threats and vulnerabilities in cloud computing. This drawback does not support the Confidentiality, Integrity and Availability (CIA) of cloud computing since cloud computing is characterized with omnipresence, elasticity and dynamic environment.

Furthermore, the specification of threats in STRIDE makes it limited for its effective application in cloud computing [13]. Cloud computing is dynamic and pervasive and cannot be threat modelled with static frameworks such as STRIDE. Additionally, defining new threats, identifying vulnerabilities and privacy related issues have not also been considered in STRIDE framework thus limiting its applicability in cloud computing. Therefore, cloud computing requires threat modelling methods which can help identify new assets and their related threats and vulnerabilities in a dynamic network such as cloud computing. Other cloud threat modelling characteristics which were less considered by most of the various frameworks include establishing user's role and estimating trustworthiness as shown in Table IV. Trustworthiness is a critical characteristic in distributed system which need to be estimated by cloud computing related threat modelling methods. In distributed computing paradigm, two or more systems with heterogeneous features and environment are combined to accomplish a given task. Assessing the security status of the individual systems to integrate them into cloud computing system would contribute towards enhancing the CIA of cloud computing [14], [47] for healthcare.

The flexibility, ubiquity and reliance of cloud computing can enable healthcare staff to access various healthcare services at different times and places. Each user sometimes has multiple roles such as an administrator with high level privileges in one domain. In another domain that user can be an ordinary user with low level privileges. Therefore, proper authorization, authentication and access control mechanisms are required to enhance the CIA of cloud computing [14], [48]. This can also contribute to complexities in scenarios where the cloud computing logs are to be analysed for users' security practices. Aside this, in the context of public cloud computing where access logs are controlled by the cloud service providers (CSP), the flexibilities for healthcare providers, as tenants, to analyse their access logs for security measures would be highly limited. In general, if tenants such as healthcare providers, require to know some information about their data which has been held in third party CSP , they might not be able to get precisely what they want at the appropriate time and this might undermined critical decision making in healthcare. From Table IV, threat modeling in pervasive computing (TMP) and Attack Tree (AT), comparatively support a higher number of cloud computing threat modelling characteristics. TMP framework support all cloud computing modeling characteristics except establishing user" role, scanning domain security, ranking and measuring vulnerabilities. TMP framework exhibited high efficiency for cloud computing based on the background that it was designed to incorporate pervasive computing environment issues [14]. For TMP to fully address cloud computing related threat modelling characteristics, it needs to be complemented with AT, AG and PTA or STRIDE as shown in Table IV. Similarly, Attack Tree (AT) also addresses more of the cloud computing threat modelling concerns but require to be completed with TMP, AG and STRIDE or PTA as shown in Table IV.

Various attack paths which can possibly be followed by attackers, can be identified by attack trees however, it does not provide detailed specific ways of exploiting resources [25, 26]. Attack graphs can be used to augment for this shortfall. TMP can also complement AT to be able to establish trustworthiness and development of counter measures [26], [27] as shown in Table IV. According to the ISO standard for healthcare security (ISO 27799:2016), healthcare organizations usually collect detailed personal information due to the ultimate importance to perfectly identify patients and correctly match them to their health records [52]. Even though other critical sectors such as the financial industries, collect demographic data, personal data, payment card details and social security numbers of their clients, the healthcare sector, additionally, collects healthcare information such as medical history, diagnosis and treatment, insurance claims and payments, bio-data and medical prescriptions. This makes the healthcare sectors' records to be greatly richer and more sensitive than other sectors including the banking and financial industry [53]. This deeply raises privacy concerns in the adoption of cloud computing in healthcare which most of the identified cloud threat modeling methods have not addressed. While adopting a synergy of methods to address cloud related issues for healthcare, privacy requirement methods such as LINDDUN should be incorporated towards identifying and mitigating security and privacy issues.

In terms of the deployment models of cloud computing, private cloud is more secure and currently fit for healthcare since the services of the private cloud computing model are usually restricted from public access and the IT Network administrators of the organization's data center are usually the cloud providers.

A. Spatial Consideration in Healthcare Domain

Current requirement in healthcare is to access patients records anywhere and at any time of which cloud computing has the ultimate solution [75]. Cloud computing can fulfil this special need thereby, providing more effectiveness and efficiency in the healthcare sector at a relatively lower cost [74], [75]. For example, cloud computing services can support hospitals in sharing EHR, doctor's references, prescriptions, insurance information, and test results [68], [69], [74], [75]. Due to huge radiology data and sharing needs, many radiology departments are already adopting cloud related methods to lower their storage costs while efficiently providing exchange of images [74], [75]. However, regulatory obstacles, privacy and security challenges are some of the barriers to adopting cloud computing in healthcare as outlined in Table I. Healthcare data specially has strict privacy and security concerns as specified in popular regulations such as HIPAA and GDPR [74], [75]. These regulatory concerns must be completely fulfilled when sensitive healthcare data is to be entrusted onto a third party such as the cloud system. To prevent exposing sensitive healthcare information to unauthorized persons, an effective and efficient security measures should be considered in the aspect of access controls, authentication, authorization, security relating to transmission and storage as outlined in Table I. That is why the threat modeling methods that should be used to threat model cloud computing for healthcare need to have all the outlined characteristics as shown in Table III, to help in identifying detailed threats and vulnerabilities in cloud computing towards providing effective and efficient counter measures. So, based on this work, various threat modeling methods such as AT, TMP, AG STRIDE or TAM can be synergiesed to cover all the threat modeling characteristics to identify detailed threats and vulnerabilities for countermeasures in cloud computing for healthcare.

B. Conclusion

It has become increasingly necessary for healthcare IT professionals to adopt to better methods of assessing the security of cloud computing towards their adoption in healthcare since healthcare data is classified among the most sensitive personal data in which the privacy and security of the data subjects cannot be taken for granted in threat modelling cloud computing for healthcare [49]. As a result, threat modelling methods for cloud computing were compared, with respect to their advantages and disadvantages. After the methods were thoroughly reviewed against cloud related threat modelling characteristics, TMP and AT threat modelling methods were found to support more threat modelling characteristics for cloud computing. Therefore, TMP could possibly be combined with AT, AG and PTA or STRIDE while Attack Tree (AT) was seen to better partner with TMP, AG and STRIDE or PTA. The challenge is that, attack tree and attack graphs are difficult to use for large sized networked systems [6], [46] because the number of possible attacks grows exponentially with the growth rate of the number of hosts [46].

In the future a development of a hybrid threat modelling framework for cloud computing in healthcare need to be considered alongside with risk identification and mitigation, and assessing the method for actual use towards enhancing healthcare security practice. Future studies need to also consider how the threat modeling methods can be incorporated into other technologies such as block-chain, towards enhancing the security and privacy of healthcare systems. Also, threat modelling methods in healthcare context need to be incorporated with privacy related threat modelling activities as found in LINDDUN [30], [50]. Meanwhile, mitigation strategies should assess some of the recent technologies [76]–[78] for adoption in cloud computing including access control measures. Additionally, cloud computing infrastructure are located across different geographical locations. This raises legal and regulatory concerns in healthcare in terms of storing healthcare sensitive data across different geographical boundaries. In the future works, there is a need to explore for the legal and regulatory ways of addressing such threats in healthcare context.

For research articles with several authors, conceptualization,Prosper Yeng Stephen Wolthusen ; methodology, Prosper Yeng and Bian Yeng; validation, Prosper Yeng., Stephen Wolthusen. and Bian Yang; formal analysis, Prosper Yeng.; writing–original draft preparation,Prosper Yeng; writing–review and editing, Prosper Yeng, Bian Yang; X.X.; supervision,Stephen Wolthusen; project administration, Bian Yang.

The authors declare no conflict of interest.

REFERENCES

[1] H.A. Aziz, A. Guled ”Cloud Computing and Healthcare Services,” J Biosens Bioelectron 7: 220,2006, doi: 10.4172/2155-6210.1000220

[2] M.U. Bokhari , Q. Makki , Y.K. Tamandani ”A Survey on Cloud Computing”. In: Aggarwal V., Bhatnagar V., Mishra D. (eds) Big Data Analytics. Advances in Intelligent Systems and Computing, vol 654.2018, Springer, Singapore

[3] Böhm, M., Leimeister, S., Riedl, C.H.R.I.S.T.O.P.H. and Krcmar, H., 2010. Cloud computing and computing evolution. Technische Universität München (TUM), Germany.

[4] P. Mell , T. Grance The NIST Definition of Cloud Computing — CSRC. NIST. 2011:1-2.

[5] IBM. Benefits of cloud computing 2019 [updated 2019-05-09; cited 2019. Available from: https://www.ibm.com/cloud/learn/benefits-of-cloud-computing.

[6] J. B. Hong ,A. Nhlabatsi , D. S. Kim, A. Hussein ,N. Fetais , K. M. Khan, ”Systematic identification of threats in the cloud: A survey”, Computer Networks. 2019;150:46-69.

[7] Healthcare, G. E. ”Centricity practice solution going beyond meaningful use.” (2010).

[8] N. Kolakowski, ”Dell practice fusion to offer medical records system. 2010”. Available from:https://www.eweek.com/news/dell-practice-fusion-to-offer-medical-records-system

[9] R. Daman, M.T. Manish, K.M. Saroj,”Security issues in cloud computing for healthcare.” In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1231-1236. IEEE, 2016.

[10] A. Shostack, ”Threat Modeling: Designing for Security: United States:”, John Wiley & Sons Ltd;p. 590,2014.

[11] L. F. B. Soares, D. A. B. Fernandes, M.M. Freire, P. R. M. Inacio, editors. Secure user authentication in cloud computing management interfaces. 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC); 2013 6-8 Dec. 2013.

[12] Modi, Krishna, and Abdul Quadir. ”Detection and Prevention of DDoS Attacks on the Cloud using Double-TCP Mechanism and HMM-based Architecture.” International Journal of Cloud Computing and Services Science 3.2:113,2014.

[13] Hamza, Yasir Ahmed, and Marwan Dahar Omar. ”Cloud computing security: abuse and nefarious use of cloud computing.” Int. J. Comput. Eng. Res 3.6: 22-27,2013

[14] A. Amini, N. Jamil, A. Ahmad, Z‘aba M. R. Threat Modeling Approaches for Securing Cloud Computin. Journal of Applied Sciences.;15:953-67,2015

[15] Hashizume K., Rosado D. G., Fernández-Medina E., Fernandez E. B. An analysis of security issues for cloud computing. Journal of Internet Services and Applications,4(1):5,2013

[16] S. M. Hashemi, A. K. Bardsiri, Cloud computing vs. grid computing. ARPN journal of systems and software, 2(5), 188-194, 2012.

[17] GeeksForGeeks. Introduction to Parallel Computing - GeeksforGeeks 2018 [updated 2018-10-04; cited 2019 02.11.2019]. Available from: https://www.geeksforgeeks.org/introduction-to-parallel-computing/.

[18] Golub G. H., Ortega J. M. Scientific computing: an introduction with parallel computing. Choice Reviews Online, 30(10):30-5637-30, 1993.

[19] Y. Jadeja, K. Modi. Cloud computing-concepts, architecture and challenges. In 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET) 2012 Mar 21 (pp. 877-880). IEEE.

[20] Ben-Yehuda O. A., Ben-Yehuda M., Schuster A., Tsafrir D. The rise of RaaS. Communications of the ACM. 2014;57(7):76-84.

[21] Lalanda P., Julie M., A., Diaconescu A. Autonomic Computing - Principles, Design and Implementation: Springer; 2013 2013-05-27. 288 p.

[22] Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.

[23] Baecker R. M. Readings in human-computer interaction : toward the year 2000. 2nd ed. ed. San Francisco: Morgan Kaufmann Publishers; 1995.

[24] Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In 2010 24th IEEE international conference on advanced information networking and applications (pp. 27-33). Ieee.

[25] hang Q., Cheng L., Boutaba R. Cloud Computing: State-of-the-art and Research Challenges. Journal of Internet Services and Applications. 2010;1:7-18.

[26] Alhebaishi N., Wang L., Singhal A. Threat Modeling for Cloud Infrastructures. ICST Transactions on Security and Safety. 2019;5:156246.

[27] Cheng Y., Du Y., Xu J., Yuan C., Xue Z., editors. Research on security evaluation of cloud computing based on attack graph. 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems; 2012 30 Oct.-1 Nov. 2012.

[28] Zimba A., Chen H., Wang Z., editors. Attack tree analysis of Man in the Cloud attacks on client device synchronization in cloud computing. 2016 2nd IEEE International Conference on Computer and Communications (ICCC); 2016 14-17 Oct. 2016.

[29] Yahya F., Walters R. J., Wills G. B., editors. Analysing threats in cloud storage. 2015 World Congress on Internet Security (WorldCIS); 2015 19-21 Oct. 2015.

[30] Gholami A., Laure E. Advanced cloud privacy threat modeling. arXiv preprint arXiv:160101500. 2016.

[31] Amini A., Jamil N., Ahmad A. R., Z‘aba M. R. Threat Modeling Approaches for Securing Cloud Computin. Journal of Applied Sciences. 2015;15(7):953-67.

[32] Malik, Nazir A., Muhammad Younus Javed, and Umar Mahmud. ”Threat modeling in pervasive computing paradigm.” 2008 New Technologies, Mobility and Security. IEEE, 2008.

[33] Zhao F., Huang H., Jin H., Zhang Q. A hybrid ranking approach to estimate vulnerability for dynamic attacks. Computers & Mathematics with Applications. 2011;62(12):4308-21.

[34] Jiang J, Ding L, Zhai E, Yu T. VRank: a context-aware approach to vulnerability scoring and ranking in SOA. In2012 IEEE Sixth International Conference on Software Security and Reliability 2012 Jun 20 (pp. 61-70). IEEE.

[35] Rhee K., Won D., Jang S.-W., Chae S., Park S. Threat modeling of a mobile device management system for secure smart work. Electronic Commerce Research. 2013;13(3):243-56.

[36] Ryan M. D. Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software. 2013;86(9):2263-8.

[37] GuiShan D, ZhengJun L, Dong Z. A security domain isolation and data exchange system based on VMM. In2009 3rd International Conference on Signal Processing and Communication Systems 2009 Sep 28 (pp. 1-5). IEEE.

[38] Jouini M., Rabai L. B. A., Aissa A. B. Classification of Security Threats in Information Systems. Procedia Computer Science. 2014;32:489-96.

[39] Zhao F., Huang H., Jin H., Zhang Q. A hybrid ranking approach to estimate vulnerability for dynamic attacks. Computers & Mathematics with Applications. 2011;62(12):4308-21.

[40] Yeng P. K., Yang B., Weyori B. A., Nimbe P., Solvoll T., editors. Web Vulnerability Measures for SMEs. Norwegian Information Security Conference; 2019 20.11.20—9; Narvik: NISK Journal; 2019.

[41] Scarfone K., Mell P. An analysis of CVSS version 2 vulnerability scoring. Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement. 1671289: IEEE Computer Society; 2009. p. 516-25.

[42] Laorden C., Sanz B., Alvarez G., Bringas P. G. A threat model approach to threats and vulnerabilities in on-line social networks. Computational Intelligence in Security for Information Systems 2010: Springer; 2010. p. 135-42.

[43] Yeng P., Yang B., Snekkenes E., editors. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC); 2019 15-19 July 2019.

[44] Nomen. (2020). Code of conduct for information security and data protection in the healthcare and care services sector. Retrieved from https://ehelse.no/normen/documents-in-english

[45] ISO. ISO 27799:2016(en), Health informatics Information security management in health using ISO/IEC 27002. 2016.

[46] Hong, Jin B., and Dong Seong Kim. ”Performance analysis of scalable attack representation models.” In IFIP International Information Security Conference, pp. 330-343. Springer, Berlin, Heidelberg, 2013.

[47] Kallath D. Trust in trusted computing - The end of security as we know it. Computer Fraud & Security. 2005;2005:4-7.

[48] Ryan M. Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software. 2013;86:2263-8.

[49] Prosper Kandabongee Yeng, Adam. S., Bian Yang, Einar Arthur Snekkenes. Framework for Healthcare Staffs' Information Security Practice Analysis: Psycho-Socio-Cultural Context. journal of Medical and Internet Research (Preprint). 2019.

[50] Deng M., Wuyts K., Scandariato R., Preneel B., Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering. 2011;16(1):3-32.

[51] Manadhata PK, Wing JM. A formal model for a system's attack surface. InMoving Target Defense 2011 (pp. 1-28). Springer, New York, NY.

[52] ISO, ISO 27799:2016(en), Health informatics:Information security management in health using ISO/IEC 27002. 2016.

[53] Yeng P, Nweke LO, Woldaregay AZ, Yang B, Snekkenes EA. Data-Driven and Artificial Intelligence (AI) Approach for Modelling and Analyzing Healthcare Security Practice: A Systematic Review.

[54] Whitten, D., 2008. The chief information security officer: An analysis of the skills required for success. Journal of Computer Information Systems, 48(3), pp.15-19.

[55] ISO, ISO 27799:2016(en), Health informatics Information security management in health using ISO/IEC 27002. 2016.

[56] Mohamed Abomhara, M.G., Geir M. Køien. A STRIDE-Based Threat Model for Telehealth Systems — NISK Journal. in Norsk Informasjonssikkerhetskonferanse. 2015. Ålesund, Norway: NISK Journal.

[57] Cagnazzo, M., Hertlein, M., Holz, T. and Pohlmann, N., 2018, April. Threat modeling for mobile health systems. In 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 314-319). IEEE.

[58] Almulhem, A., 2012. Threat modeling for electronic health record systems. Journal of medical systems, 36(5), pp.2921-2926.

[59] Deng, M., Petkovic, M., Nalin, M. and Baroni, I., 2011, July. A Home Healthcare System in the Cloud–Addressing Security and Privacy Challenges. In 2011 IEEE 4th International Conference on Cloud Computing (pp. 549-556). IEEE.

[60] Satyanarayanan, M., 2017. The emergence of edge computing. Computer, 50(1), pp.30-39.

[61] Aazam, M. and Huh, E.N., 2014, August. Fog computing and smart gateway based communication for cloud of things. In 2014 International Conference on Future Internet of Things and Cloud (pp. 464-470). IEEE

[62] Opara-Martins, J., Sahandi, R. and Tian, F., 2016. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. Journal of Cloud Computing, 5(1), p.4.

[63] German Hospital Hacked, Patient Taken to Another City Dies, https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies, Date: 17/09/2020

[64] HEALTH SHARE OF OREGON: 654,000 PATIENTS. Accessed on 24/09/2020. https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far

[65] Luke Irwin,Breach at Norway's largest healthcare authority was a disaster waiting to happen Date: 01/02/2018, https://www.itgovernance.eu/blog/en/breach-at-norways-largest-healthcare-authority-was-a-disaster-waiting-to-happen

[66] Michael Usiagwu is an Entrepreneur, 6 Cloud Security Threats Healthcare Companies May Face – With Solutions, Date: July 14 2020: https://www.tripwire.com/state-of-security/featured/6-cloud-security-threats-healthcare-companies-face-solutions/

[67] European Commission, ”What rules apply if my organisation transfers data outside the EU?”, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en

[68] Brad Taylor,”Healthcare organizations and the cloud: Benefits, risks, and security best practices”,Accessed on 25/09/2020 https://www.helpnetsecurity.com/2018/01/02/healthcare-cloud-risks/

[69] COMPLIANCE, NETWORK SECURITY, NEWS, ”Misconfiguration is the Most Common Cause of Healthcare System Breaches”, Accessed on 28.09.2020,https://mytechdecisions.com/compliance/healthcare-system-breaches/

[70] Almulhem, A., 2012. Threat modeling for electronic health record systems. Journal of medical systems, 36(5), pp.2921-2926.

[71] Papa, S.M. and Casper, W.D., 2011. Levels of Trust.

[72] Conrad, E., Misenar, S. and Feldman, J., 2010. CISSP study guide. Syngress.

[73] Yeng, P., Yang, B., Solvoll, T., Nimbe, P. and Weyori, B.A., 2019. Web Vulnerability Measures for SMEs.

[74] Terry, K. (2012). Cloud computing in healthcare: the question is not if, but when. Retrieved from http://www.fiercehealthit.com/story/ cloud-computing-healthcare-question-not-if-when/2020-10-21

[75] Ahuja SP, Mani S, Zambrano J. A survey of the state of cloud computing in healthcare. Network and Communication Technologies. 2012 Dec 1;1(2):12.

[76] Chinnasamy P, Deepalakshmi P. A scalable multilabel-based access control as a service for the cloud (SMBACaaS). Transactions on Emerging Telecommunications Technologies. 2018 Aug;29(8):e3458.

[77] Chinnasamy P, Deepalakshmi P, Shankar K. An analysis of security access control on healthcare records in the cloud. InIntelligent Data Security Solutions for e-Health Applications 2020 Jan 1 (pp. 113-130). Academic Press.

[78] Chinnasamy P, Deepalakshmi P. Design of Secure Storage for Healthcare Cloud using Hybrid Cryptography. In2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) 2018 Apr 20 (pp. 1717-1720). IEEE.