Research Article

iMedPub Journals
www.imedpub.com

Journal of Hospital & Medical Management
2471-9781

2021
Vol.7 No.5:273

A Study of Cybersecurity Framework for Healthcare Internet of Thing Systems

Shiva Kiran Nallaga[1], Vidyavati Ramteke[2], Manda Sundeep Kumar[3]*

1 Symbiosis Centre for Information Technology, India
2 Assistant Professor, Symbiosis Centre for Information TechnologySymbiosis International (Deemed University), Pune
3 Mvgr College of Engineering, Viziyanagaram, India

***Corresponding author:**
Manda Sundeep Kumar

sundeepkumar378@gmail.com

Tel: +7908261005

Mvgr College of Engineering, Viziyanagaram, India

Citation: Nallaga SK, Ramteke V, Kumar MS (2021) A Study of Cybersecurity Framework for Healthcare Internet of Thing Systems. J Hosp Med Manage Vol.7 No.5:273.

Abstract

As with any technical innovation in culture, many will still use it to their own gain when new opportunities emerge. Current Internet of Things (IoT) applications have particular protection vulnerabilities owing primarily to their complexities and variability of technologies and data. This could not incorporate the risks resulting from these IoT networks within an established risk structure. And outside the technology nomenclature, cyber security is as important to our society as the application itself. They cannot really be divided: the innovations on which we depend every day today decide our society, our national security and therefore the nature of our society. As they connect this healthcare system to the network through the Internet, the software is susceptible to many cyber threats and security initiatives. A secure protection framework cannot impede basic security aspects such as authentication, anonymity, availability, accessibility and non-repudiation. This paper discusses improved constructive security against dynamic and inventive threats against critical health infrastructures. They recommend a comprehensive solution to cyber-attacks through an interconnected system of knowledge security. To model and test this method by designing and checking the adaptive technique for defense and attack.

Keywords: Cybersecurity, Healthcare, Adaptive security, Machine learning, Internet of Things, Smart home

Received: April 17, 2021, **Accepted:** April 21, 2021, **Published:** May 18, 2021

Introduction

Cyber-attacks are a today's fast-increasing problem in all key technology industries. In the health sector, cyber attacks are of great interest because these attacks will actively endanger not only the protection of our infrastructure and records but also American patients' health and safety. In the health sector, it is under constant cyber-attack and no organization can avoid this. While creativity in health information technology contributes to hope and growing maturity of health Science, our technology can only function for us if it's healthy, and it can help to tackle some of our most difficult concerns, whether in clinical care, medical testing, public health or health system growth. Information technologies are critical for the healthcare system now and future, and so we ought to undertake every workable action to secure them. Besides hospitals and primary care physician offices, the health system will involve sensor networks within intelligent houses and wearables placed on patients. This turns health systems into diverse settings that are heavily dispersed, **(Figure 1)**. Combining clinics, healthcare facilities, smart houses and different portable nursing appliances, healthcare systems and infrastructures is being complex, automated and integrated more than ever before. These facilities are also susceptible to a range of new cyber-attacks.

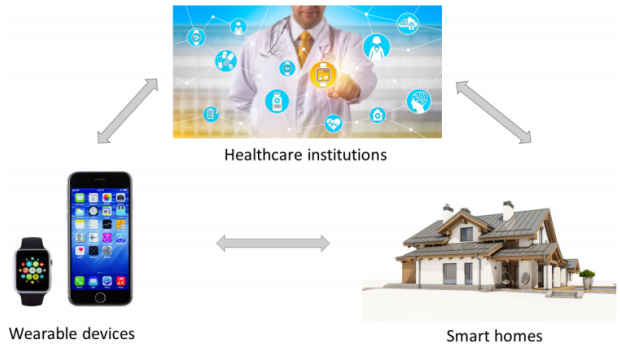

Figure 1 Healthcare IoT Platform may include healthcare institutions, smart homes, and wearable devices with smart phones serving as gateways.

The automated technologies are gradually at the expense of

privacy. There seems to be an implicit balance, because although we recognize any misuse of the data we hold, it remains a vital foundation block in our culture and must lead to every remedy. It is realize that there is no 100% safe device, and all sensitive details kept on every computer, whether the government, the company or otherwise could be infringed and private details publicly disclosed.

Although interconnecting these devices provides several advantages, it also brings protection problems which may affect data security and integrity [1]. Security indicators will provide companies with a tool to test and consider their systems' protection status since attackers often search the weakest link [2]. Clinicians and other healthcare practitioners may not see protection from the same angle as Medical professionals and are motivated solely by the desire to offer an outstanding service for patients [3]. Protection initiatives will help customers learn about their company's experiences and patterns and test how the enterprise does among their business peers [4]. In recent years the healthcare industry has undergone several security threats and the frequency has escalated. According to a new Verizon data survey, the amount of safety infringements in the healthcare sector has risen considerably from the previous year, with 85% of malware in the Ransomware market targeting this business.

To secure their resources, the vital infrastructures of IoT-enabled healthcare need advanced cyber defenses. These systems must be scalable, resilient, stable, and capable of detecting a wide spectrum of risks and taking wise decisions in proper time. To meet the complexities of ensuring their stability and durability, a comprehensive technology architecture for the safety of diverse health care environments is essential. Resilience, performance, protection and privacy are major problems and pose problems, it applies particularly where integrated physical and cyber risks to complex health environments. Facing massive measures to protect critical IoT networks, many remain unintendedly exposed to take cyber-attack. Dynamic attackers can change their approaches to the security environment and two measures recently introduced. The device must also secure IoT data that needs critical creation and adaptation in IoT protection. This analysis gains additional information to improve dramatically the quality and productivity of adaptive protection in the prevention of IoT adaptive attacks. This is done by[1] modeling and testing the mechanisms of adaptive attack and protection.

[2] Development of adaptive attack quantitative security mechanisms using mathematical calculation and [3] performance simulation tests and assessments using appropriate simulation techniques, e.g. multi agent systems and system dynamics.

Earlier, it introduced an evolutionary game framework [4,5] for modeling adaptive attacks and data integrity protections for advanced measurement infrastructures. In this article, we [1] present large building blocks of a complex IoT healthcare cyber protection architecture which is focused technically on machine learning and [2] simulate and test this system by modeling and testing the adaptive attack-defense strategy.

Background Works

In [6] the authors dealt with creating a multi-source anonymized medical database. To achieve data convergence within a heterogeneous environment comprising multiple healthcare facilities, this issue author presented the approach thus protecting data efficiency and patient confidentiality. First, to store and share patient information for the diagnosis, the author recommended a stable and modular cloud eHealth system. Second, RSBD algorithm for accurate collection of health data separately from various sources for testing.

In [7] the writers address the Health Information System (HIS) general definition of privacy, since most HISs are accessible online. The inconsistencies in identity, protection and such relevant works in HIS and user feedback will secure their identity. In [8] the authors suggested 'PriGen;' a generalized structure that protects the secrecy of critical cloud data. PriGen helps consumers to safeguard privacy against third party support when using cloud-based healthcare facilities. The homomorphic encryption feature on sensitive private data protects the secrecy of the private information submitted by cloud customers to insecure cloud-based healthcare services.

In [9] the author 'aim is to validate and address security-privacy concerns in delivering medical care everywhere. They analyse current frameworks, explore the regulation, structural and cross-country policy problems to resolve the related protection and privacy concerns, and categorize these issues in terms of consumers, websites, communications and computers. A coordinated initiative by scientific, human and social science organizations may react effectively to the core questions of privacy protection at all periods in this alternative model of healthcare. In [10] the scientists showed a study of the privacy models for the attack, affiliation discloser attack and attribute discloser attack. They also addressed the collection of templates and methods in multiple discloser attacks used to reveal patient data.

Consideration of three forms of activities most applicable to health ML development: scientific, organizational and epidemiological. Health activities include the assessment, operation and examination of patients, typically carried out by trained health care professionals, for example, the confirmation of the diagnostic process. Operational tasks are operations similar to therapeutic duties, but which are important or useful in the procurement of care, for example, the production, preservation and retrieval of medical records. Eventually, epidemiological activities refer to the detailed assessment of the health concerns and results of a community of individuals in a specific population. An analogy is the implementation of a disease epidemic alert device. Since they connect epidemiological applications of ML to improving people's capacity to determine in the other categories mentioned here (clinical or functional), there is no sign of perfect computation for epidemiological activities that have any other performance than advising a human judgment.

The NASSS project and other studies in emerging health infrastructure delivery research underlines the relevance of discussing the benefit proposition of a modern system for healthcare stakeholders. For various stakeholder classes,

the benefit proposition of emerging technology can vary. Deployment mechanisms explicitly discuss the impact of disruptive innovations on consumers, health care professionals, administrators and politicians, among others. The therapeutic, financial and epidemiological role kinds described may lead to separate benefit recommendations for the various stakeholder classes, which implies that implementations of ML which favour one community over another, for example by defining an internal scheduling mechanism to optimize cost effectiveness might be helpful to administrators rather than health care practitioners. Identifying the discrepancies in value recommendations for the different parties taking part in the application of ML is a significant factor for efficient acceptance and usage.

The benefits of an ML system delivering decision making vs an automation service are different and require multiple forms of deployment problems. The design of decision support structures in public health care that do not incorporate ML technologies has been well documented and the issues involve limited control, time constraints and user experience frustration. Development projects involving ML decision support systems may involve analysis of previous experience to build development methods to overcome the identified challenges more effectively. They expect automation deployment projects to encounter a range of common and distinct obstacles.

For example, opinions of stakeholders on implementing autonomous robots into several healthy environments have shown a general lack of concern, awareness and anxiety of how the practice is interrupted and dispersed. While automation has occurred across technology such as cardiac testing for decades in health care, the question of how appropriate stakeholders interpret emerging ways of automation remains a significant topic. This argument poses the general question of automation that ML implementations will offer, relevant to uncertainty whether ML can either improve or eliminate the function of health care professionals.

Any device must satisfy the security needs to protect the data secure.

A. Authentication: Authentication is a mechanism where a system tests the character of a person who needs to access it. It is known as a chief defense.

B. Integrity: the intruder can change or update No data or information during transmission. The framework must have 100% data confidentiality, thus improving the confidence level.

C. Confidentiality: it ensures that the intruder has no unauthorized access to details.

D. Availability: Access to data must be given whereby the legal users. It should not withhold details to authentic people.

The system focuses on functional simulations in the healthcare IoT and models for flexible and complex attackers and defenders. They must test assailant templates against actual cases and scenarios. An efficient processing defender must surpass conventional static defensive strategies dramatically and battle adaptive aggressor strategies. Using evolutionary defense algorithms in Healthcare, IoT needs practical examples of tactics for attackers and supporters. This may determine how these techniques are suited to the opponent 'behaviour. It must also treat the world as a multi-agency setting because various attackers and defenders will coexist and collaborate. The creation of these models thus involves a critical mix of statistical analysis, game theory, dynamics and real-life safety cases and scenarios. There are established drawbacks of machine learning as applied of multi-agent contexts

A. Adaptive Attack Approaches Model

For adaptive attack tactics, many opponents target an IoT medical infrastructure in order to adversely affect the secrecy or to alter information for them, i.e. change, replicate or insert false information. We have to measure the losses and their subsequent benefits to model attack patterns. Attack costs and benefits can differ based on attack forms and data sites and equipment.

B. Adaptive Security Policy Models

This considers many components to model adaptive security strategies that reflect different sensors, wearables, smart homes and networks of medical institutions, and shape an IoT structure of healthcare. To construct security plans, protection expenses and damages must be quantified where security interventions have declined. These values rely on the position and types of information.

C. Attack-defense mechanism simulation and review

The evolutionary mechanisms of competitive assault and response have several similarities in biology and in humanities. Dynamics of the method.

Customarily used for modelling structures in all these fields, it is a perfect candidate to generate ideal models for evolutionary adaptive attack-defense applications. To improve these models, we may explain relationships between various subsystems, particularly definitions of permissible and malicious behaviour. As cyber-attacks grow complexity, the major factors driving growing corporate cyber protection include:

1. Absence of C-level web governance expertise. Executives cannot allow improvements in organizational protection policy quickly. Such reforms will secure organizational capital against the continuously changing and complex existence of today's cyber threats. The worst aspect is that cyber-criminals may not rob companies of their C-level ethos and that cyber-security is constantly at a problem for management review meetings.
2. Ways to use state-of-the-art identification tools for cybersecurity. Current database systems allow data crushing more effective as the data needed for cybersecurity research is accessible concurrently. This practice includes developed strategies for cryptography research, including artificial learning, data mining and information exploration. Data mining is a subcomponent of information exploration where the data are retrieved in a particular series of steps. Information exploration involves data cleaning, collection and implementing, previous expertise and existing analysis techniques. Machine learning and data mining differ when

they use identical techniques and approaches. Although machine learning is based on classifying data samples and predicting occurrences and activities, it concentrates data mining on the identification of previously unknown trends in data (very close to zero-day cyber assault detection). Implementing these strategies is now one of the major forces for organisations, like cyber protection, to accomplish their targets.

3. Fragmented systems for cybersecurity. While possessing a vast range of mechanisms to protect the infrastructure of an enterprise against cyber threats, it remains a very challenging problem for policymakers in cyber protection. Some sectors, including the insurance industry, may not have an acceptable model to adopt to ensure the cybersecurity. This is partly because of the absence of customer data to create legal and fraudulent profiles to which computer education or AI techniques may be adhered; fraud concepts vary in the insurance industry and the banking sector. In the former situation, insurers are primarily worried that products are initiated with no previous awareness of the clients and work in a fractured regulatory setting. For example, the insurance sector, unlike banking, is not tightly controlled in the US, burdening the implementation of cyber protection against silver bullet strategies, since they rely constantly on regulation. Even without the industry-specific cybersecurity context, cybersecurity targets are hampered throughout different industries.

Materials and Methods

A simulation illustration has been applied and tested to illustrate the adaptability of the complex system to cyber threats **(Figure 2)**.

We recognize the following nodes as a Healthcare IoT system: one Healthcare institution, three smart homes and two smartphones. Figure 2 shows the configuration of this device. Smart Phone 1 and Smart Phone 2 capture wearable tracker info. Smart Home 1 gathers details from three wearables, Smart Home 2 gathers information from two wearables, and Smart Mobile 3 gathers details about two wearables and Smart Phone 2 collects data from two wearables. Both smart homes and smartphones 1 transmit their data to Healthcare Institution directly, and Smart Phone 2 transmit the information gathered to Smart Home 3**.**

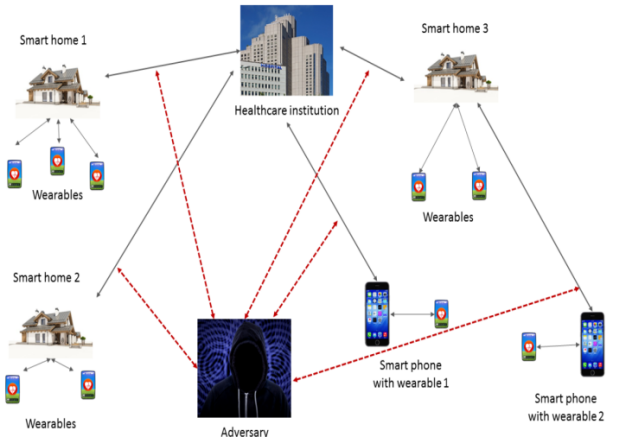

Figure 2 Topology of Adaptive Cybersecurity Framework for Healthcare IoT.

We therefore presume that perhaps the attacker will target any device node, and if the data gathered by this node is vulnerable, they are vulnerable. To intercept or interrupt data sent from either node, the opponent will either explicitly target or attack his parent node. We add the ident (i) feature for each node (ii) to return a collection of children for that node.

The security costs and attack costs for each node of the device are represented by c^d_i and c^a_i, accordingly. The data got as a meaning. To calculate these values, an asset value $v(i)$ is specified for each node. These values are automatically chosen for this simulation. We may quantify these values for specific networks through every reasonable form of risk evaluation. We list the parameters on **(Table 1).** The adversary will switch from various attack levels. The set is described by $S = s_0; s_1;.....s_p$. We describe a range of security seriousness levels equivalent to the attack levels as $D = d_0; d_1; ..... d_p$. We identify four potential levels of attack and protection in this context. We set the following values to: 0% (not secured), 33.3%, 66.6% and 100% (fully secure). The attacker strategy area K and the security strategy region M comprise all workable variations of the attack and protection levels around the node range.

Table 1: System parameters for healthcare IoT example.

Node	$v(i)$	c^a_i	c^d_i	r^*_d	r^*_a
Healthcare institution	80	16	4	0.39	0.48
Smart Home 1	30	6	1.5	0.13	0.10
Smart Home 2	30	4	1	0.12	0.10
Smart Home 3	20	4	1	0.11	0.11
Smart Phone 1	10	2	0.5	0.11	0.09
Smart Phone 2	10	2	0.5	0.10	0.10

Stochastic Attack-Defense Game Model:

Figure 2 shows the mapping partnership between cyber-attack-defense and stochastic game model. It composes the stochastic system of an attack-defense system and a switch between states inside each state. It is presumed that the two key elements "knowledge" and "game order." Restricted by minimal reasoning, the attacker's past behaviour and the reward roles of the attacker are classified as private information of the attacker **(Figure 3).**

We provide a high-level overview of our current strategy to create an individual IoT security solution that involves annoyance, recognition, learning and lateral movement. Figure 4 displays the engine diagram. The engine will simulate IoT network topology and produce the attack-graph from the host's configuration (e.g. machines, devices, operating systems, software, firewalls, servers, routers). The attack graph links two nodes V1 and V2 where there's a channel, a protocol and a compromised V2 program that can jeopardize V2 on V1. The engine provides a search feature to find new vulnerabilities in public databases of vulnerabilities, including the National Vulnerability Database (NVD) [11]. If we have found a new weakness, the attack network is modified by inserting new network edges. To exploit the vulnerability, we use the Standard Vulnerability Scoring System (CVSS) [12] to determine how the attacker will reach the vulnerability and

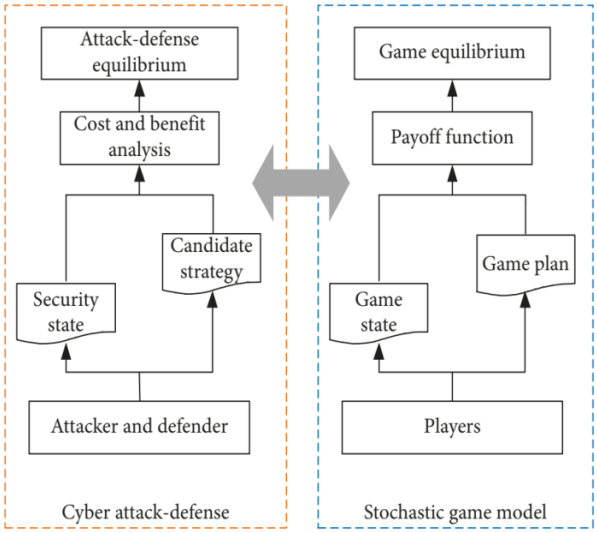

Figure 3 Mapping relationship between cyber-attack-defense and stochastic game model.

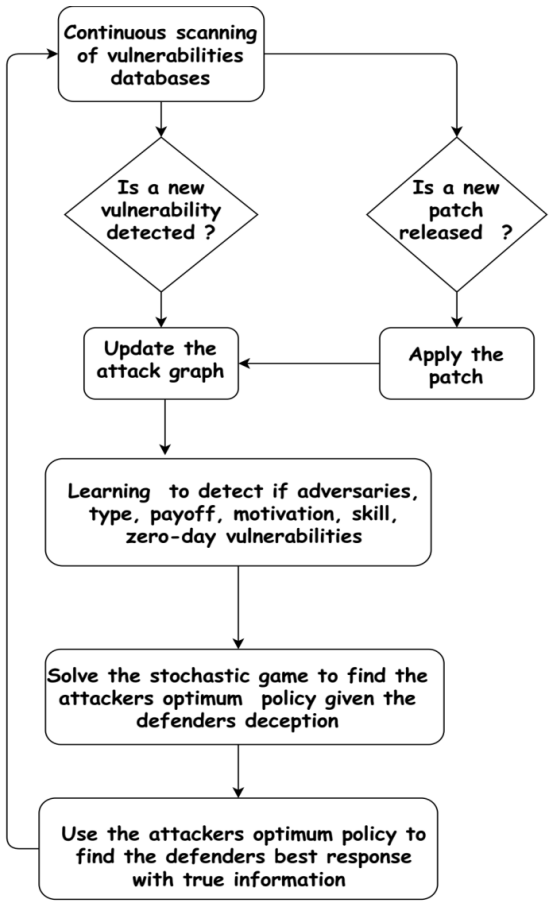

Figure 4 Best response engine for self-secured systems.

its difficulty, and how many times (if any) the attacker requires verifying. When a new patch is issued from NVD, the device immediately applies the patch and changes the threat graph to the patched exploit **(Figure 4).**

We apply a complex cyber manipulation system until we identify an intrusion to confuse the attacker and to reduce the effect of the intruder on the IoT network. We build a rigorous method for smart exploitation to identify these attacker features: reward, incentive, power, and zero-day vulnerabilities, not in the NVD database. The learning algorithm has to converge rapidly to be consistent with frequent shifts in network topologies.

When an adversary is identified, a stochastic two-player game illustrates the relations between the intruder and the defender. In the game, the states reflect the attack-graph nodes, and the transformations refer to the edge-vulnerabilities that the intruder will use to shift sideways. The response to the game offers the offender the right strategy of annoyance. Provided the ideal strategy of the attacker, the best response of the defender is determined using exact facts. The best solution in either state of play would cause the process to stabilize easily in a secure situation. The framework follows the best solution to isolate insecure systems or dynamically update them, thus reducing the advancement of the assault at each device node. Ultimately, constant vulnerability in learning and testing helps the device to respond to recent attacks.

Summary and Discussion

In the section on cyber security steps, we grouped the indicators into several groups to quantify the security of devices and support informed decisions by policy makers. We talked about healthcare issues and agreed this might help ease some cyber threats by improving protection mitigation systems and instilling the positive safety culture in these organizations. Even though these steps can be utilized in any organization, they are particularly well-suited for clinical practice where the end devices are complicated and where, because of existing processes and embedded medical equipment, the threat surfaces are greater. This metrics can have an overall safety exposure when measured and enable system engineers to respond quickly to close gaps. In the development process, measures such as those for Red teaming may often be used during implementing new protection technologies by evaluating the protection defenses of these projects.

Security vulnerabilities in modern IoT systems analyze cyber risk assessment:

Owing to the vulnerability of weaknesses in current IoT networks, cyber risk management mechanisms, risk vectors and risk rankings are essential to test critically. We address the cyber-risks relevant to IoT and IoT networks in this report. We also provided a crucial overview of the Mechanisms for cyber security risk evaluation, their problems and insights for the future, concentrating on the industrial and healthcare industries, particularly the Internet of Medical Stuff (IoMT). Developing a cyber-risk theoretical method for IoT systems is among the purposes of this project. Based on literature and study, it developed a computational method to measure cyber-attack for IoT systems and take into account the IoT-specific variables. These parameters were used to measure the risk effect and chance of IoMT systems. The formulas measure the risk score and determine the (high, medium, low) risk rate of IoMT instruments. IoMT systems actively affect and support

human life by the availability of resources for clinical tracking and life-saving equipment.

The first phase of risk management involves of assessing the risks to an IoT asset to be identified and the intrinsic danger and its effects evaluation. Danger affects include high, medium and low scores. For starters, a "high" impact rating shows that the effect may be important. Medium shows that the effect will negative, however recoverable, and/or unpleasant. Low is where the effect is small or non-existent. The next step is to assess the probability of the hack, taking into consideration the organization's control system. Examples of chance scores are:

High — the root of the danger is strongly driven and adequately sensitive, and defends are inadequate to mitigate the vulnerability.

Medium–the root of the risk is driven and willing, but there are safeguards that may discourage effective vulnerability.

Low–the root of the risk lacks incentive or power or controls to discourage or at least hinder the exercise of vulnerability.

Conclusion

Cyber attack is a challenge for all businesses and not only for hygiene, but has a much greater impact when it affects public safety. The remarkable growth of devices and network smartness determines technological well-being. As the works are shared and managed intelligently, security plays an important role in maintaining the author's credibility. The challenges in health service, processes and society were discussed. In this paper, we introduced the key components of a dynamic computer security system of the IoT network.

References

1. Smith C (2018) Cybersecurity implications in an interconnected healthcare system. Front Health Serv Manage 35: 37-40.
2. Coventry L, Branley D (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113: 48-52.
3. R. Koppel, S. W. Smith, J. Blythe, and V. Kothari. (2015) Workarounds to computer access in healthcare organizations: you want my password or a dead patient? Book title=ITCH 215–220.
4. Savola RM, Savolainen P, Evesti A, Abie H, Sihvonen M (2015) Risk driven security metrics development for an e-health IoT application- in 2015 Information Security for South Africa (ISSA). IEEE1–6.
5. Svetlana Boudko and HabtamuAbie. An evolutionary game for integrity attacks and defences for advanced metering infrastructure. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (ECSA '18). ACM, New York, NY, USA, Article 7-58.
6. Dubovitskaya, Alevtina, Visara, Matteo, Karl, et al. (2015) A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration. IFIP Advances in Information and Communication Technology.
7. Bindahman, Salah, Zakaria, Nasriah (2011) Privacy in Health Information Systems: A Review. Communications in Computer and Information Science.
8. Rahman, Farzana, Ahamed, Sheikh, Yang, et al. (2013) PriGen: A Generic Framework to Preserve Privacy of Healthcare Data in the Cloud.
9. Mohd Anwar, James Joshi, Joseph Tan (2015) Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. Health Policy and Technology 4: 299-311.
10. 10.Lina A, Abuwardih, Wa'ed Shatnawi, Ahmed Aleroud (2016) Privacy preserving data mining on published data in healthcare: A survey: 1-6.
11. Booth, Harold, Doug Rike, Gregory A Witte (2013) "The national vulnerability database (nvd).
12. Mell, Peter, Karen Scarfone Sasha Romanosky (2006) "Common vulnerability scoring system." IEEE Secur Priv 4: 85-89.