An Ontological Framework for Healthcare Web Applications Security

Mamdouh Alenezi
College of Computer and Information Sciences
Prince Sultan University, Riyadh
Kingdom of Saudi Arabia

***Abstract*—The current era of digitization and transformation causes various issues and advantages both at the same time in the healthcare sector. The beneficial advantages are exceptionally good but the issues that are gardening the business of attackers is a serious issue and requires effective prevention. Current statistics and attack vector analysis portray that technical breaches have the most common and highest priority in numbers. This type of information opens a need to prevent and develop an effective model that helps to exerts and healthcare practitioners in security management. In order to achieve this desired goal, we adopt and apply an ontology-based approach of security and development methodology and provide a model that effectively produces systematic secure pathways to design healthcare web applications. The conceptual framework discussed in the study has many effective and beneficial advantages namely, it gives a unified pathway to future developers; the model also attains focus on requirement identification during development and portrays its significance.**

Keywords*—Security; web application; healthcare; digitization; requirement

I. Introduction

The era of digitization led to the whole concept of businesses and services on a virtual platform. This type of transformation creates an exceptionally beneficial environment of working. It is unified that digitization has various beneficial and good effects for current businesses and services but there are also some adverse effects available that tell us about the possibility of exploitation and digital systems and the impact of harm after exploitations. It is very significant and necessary to investigate and facilitate models that reduce the possibility of exploitation in systems.

This type of exploitation possibility and attack situations raise the requirement of a solid and secure fundamental concept of security in web application security. These types of exploitations and attacks pose some serious harm and defects in the web application that cause serious harm for hosting organizations and businesses [1]. Any type of exploitation and vulnerability creates an adverse reputation situation for business because users do not want a type of interruption or loss of data during the use of web application and if it causes then the reputation of the application and its owner gets affected. Now, it is frequently shown that this type of exploitation possibilities and issues appeared only because of any type of flaw and vulnerability in the application.

Most of the time these vulnerabilities and flaws are overlooked by the development team because of the deadline and hurry issue [2]. Further, many of the organizations do not identify which factors need attention for security or which not. However, from some previous years, many researchers and experts are paying attention to factors that need considerable attention for security in software and web application and in this proposed article we are also paying attention to them. Web application security is something that associates the whole development functionality of it when we talk about its security. Security is something that can only be achieved by systematic security towards development in web applications [3]. Producing a secure development and development towards systematic security is something that demands an appropriate equipped team and laboratory.

To make this development and its system more clear and efficient SHIELDS discusses a secure development project that discusses various security models and models them towards web application security. This project opens a door for repositories that effectively help secure development by providing the best expert practices and their processes. This type of project is effective and systematic but unable to give foundation security functionality in web applications. The development of security is something that demands implementation from the basic level of development phases. To make it possible discussing and providing an artifact-based approach that gives an effective result is required.

The proposed paper tries to present a systematic step-wise framework based on the secure development of healthcare web applications from an ontology perspective. Ontology is nothing but a novel systematic idea or concept that has some exceptionally effective potential to portray solid and effective results. The proposed model in the paper associates security factors from basic development phases and tries to manage them systematically further. The proposed model in the paper is a conceptual ontology-based model that aims to provide effective and secure development for web applications.

II. Materials and Methods

A. Relevant Literature Analysis

Semantic analysis and its tools provide support to ontology-based security modeling and help them in achieving their goals. The concept of ontology makes them very specific and conceptual [4]. Searching the ontology-related literature for security perspective is not so hard due to its wide adaptation.

However, it is surprisingly challenging for authors to get a relevant healthcare web application development-based ontology approach. After a long and exhausting literature search, we could not find any specific literature based on ontology that talks about artifacts and other functional security attributes of development phases. To summarize other studies that associate the ontology concept effectively and discuss it towards security in various other parts similar field, we discuss some literature below:

In order to secure the software by adopting the ontology concept, researchers proposed a model by associating the SecEval framework and managing it towards software security [1]. The researchers combine the developed model with software engineering approaches and produce some effective results as an outcome. This literature motivates authors of the proposed work to choose the ontology for web application security.

As the next relevant study, we find an article that extensively manages various factors of the possible risk that cause bad influence on software security and manage them through various models discussed in the paper [2]. This type of model manages the risk and provides long serviceability as well as security in software. The result discussed in the paper has potential and good efficiency.

Further, as a case study, a research study associates ontology-based security modeling for user perspective and models their possible threads and its perspective [3]. Moreover, to facilitate software development security a study summarizes the facts of security modeling from an ontology perspective and gives an extensive analysis of them [4]. The results discussed in this article are effective and sensitive.

Furthermore, to provide development knowledge security and management the relevant study talks about various contexts-based security artifacts and their features respectively [5]. This type of model provides a contextual ontology approach that produces effective results.

The above-discussed literature discusses various perspectives and previous use of ontology. We try to understand their work properly and then portray an appropriate model that has novel utilities and working processes. It is very significant to adopt ontology in secure healthcare web application development because there is no specific work available currently that talks about web application security in healthcare or normally about any web application context.

B. Needs for Ontology-Based Model

Healthcare is a sector that deals with sensitive and huge amounts of data. It is a challenging and crucial task for experts to manage and secure the whole healthcare data management and web application properly due to its complexities. The digitization era forces healthcare services to be digitized via various online platforms and web applications. In such situations, it is very important to apply security strategies and processes efficiently. Before discussing the proposed model and idea it is an important job to talk about the origin of the idea and its need in a relevant field.

Healthcare web applications are applications that get penetrated frequently by attackers in current situations. Due to the sensitivity and value of health information, it is very normal and frequent for attackers to target and exploit healthcare web applications for valuable information breaches. A survey about healthcare data breach victims tells that the amount of victims from 2005 to 2019 is 249.09 million. Further, 157.40 million are affected only in the last few years [6]. Now, if we look beyond the reported attack scenario of data breach attacks the total number of attacks implemented and registered with governing bodies are 2216 from all around the 65 countries of word, and 536 breaches are from the healthcare industry in all of them. This type of statistics portrays the severity of the healthcare sector and gives an understanding that healthcare is the most targeted and sensitive field for attacks [7].

Moreover, there are a lot of breach-related statistics for healthcare web applications are available like: a report published by IBM in 2019 shows that the average revenue loss caused by attacks in all the fields and world is around 3.92 million dollars and if we look at the healthcare field specifically then the cost of a breach was 6.45 million dollars [8]. These statistics are automatically sufficient to portray the sensitivity and thread on healthcare web application security. Managing these issues and problems of healthcare is the most prioritized and immense demand of the situation.

To understand the previous healthcare records and breach statistics, we provide Table I and Fig. 1 which contain data related to previous year records and the data breach counts. This table portrays that healthcare data attacks are increasing day by day. The increasing use of web applications for providing health services creates a sensitive condition for security measures because of the complex nature of healthcare it is very challenging to manage every possible security measure on web applications. Attackers attain these loopholes as their weapons and target the system effectively and exploit the system on a large scale.

TABLE I. PREVIOUS ATTACK STATISTICS

Breach Year	**Count**	**Amount of Data (In Millions)**
2010	199	5.530
2011	200	13.150
2012	217	2.800
2013	278	6.950
2014	314	17.450
2015	269	113.270
2016	327	16.400
2017	359	5.100
2018	365	33.200
2019	505	41.200
Total	3033	255.18

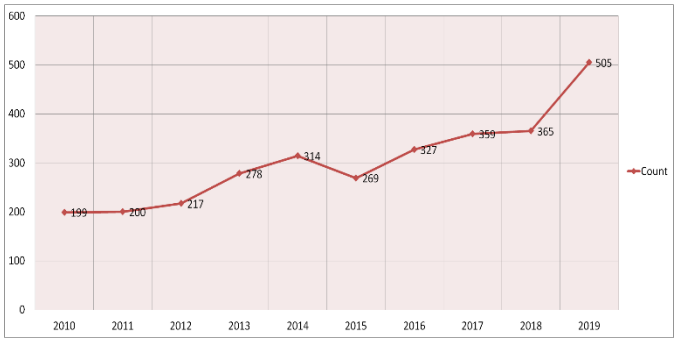

Fig. 1. Graphical Attack Illustration.

Table I and Fig. 1 portray data summarized and associated by HIPPA [9, 10]. The summarized information about the number of breach incidents and the number of breach records is totally surprising because these are officially registered and known cyber-attacks implemented on healthcare organizations. The amount of breach records is very high and significant because health is something that is totally and directly connected to the life of humans. A breach in this type of data can cause some serious life-threatening situations to the patients. Therefore, it is an immense need to manage web application security and attain security for healthcare.

Moreover, after understanding the attack statistics in healthcare it is a significant job to remediate its issues. To identify issues, it is necessary to find the loopholes first for healthcare breach incidents. To make it simple, we portray the various sources of breach registered and identified by experts in the following Table II. The following table represents the specific counts of breach incidents executed by any specific source that gives a clear point-wise understanding of healthcare loopholes and helps the experts to prepare preventive measures.

In Table II, it is clearly described and represented that technical issues are the most common and frequent exploit creators in healthcare. However, if we look at both Tables I and II comparatively then the data analysis tells that web application vulnerabilities cause maximum issues and exploits in healthcare in need of an instant solution. Thus, it is evident that technical faults cause and create issues in the current era and attackers grab these issues as an advantage and inject applications of healthcare very frequently on a large scale.

All in all, the whole statistics and attack data represented in this paper portray the current serious and sensitive situation of healthcare web application management as well as it also poses the need and requirement of functionality-based security measures that pillar the security of healthcare digitization from the deep down bottom. That is why the proposed article effectively aims to apply an ontology-based model that gives additional affectivity and conceptual understanding to the experts about how to build healthcare web applications.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar.

C. Adopted Ontology-Based Idea

As stated in the introduction ontology is something that portrays conceptual systematic steps that help in producing a secure and systematic manner of process and development methodology. In the development context of healthcare web application ontology adaptation is a novel that is why it is important to draw a proper connection between ontology concept and healthcare web application development. Developing a context-based model for effective security and efficiency in any type of process can only be achieved from ontology ideas [2].

Ontology ideology and concept are universally adopted and used in various fields like new mobile communication development and real human-machine interaction, etc. [11-15]. Ontology is nothing but simply a conceptual relationship of two ideas on one platform. This type of approach helps experts to relate the real live world issues into machine scenarios and portray or solve them through machines. Following figure 2 portrays the adopted ideology of ontology and tries to portray an overview of working.

TABLE II. SOURCE BASED ATTACK STATISTICS

Year	Technical Issues & Causes	Human Error & Disclosure	Theft	Miss Handling
2010	8	8	148	10
2011	17	27	136	7
2012	16	25	138	8
2013	25	64	150	13
2014	35	76	143	12
2015	57	101	105	6
2016	113	129	78	7
2017	147	128	73	11
2018	158	143	55	9
2019	274	142	51	7
Total	**850**	**843**	**1077**	**90**

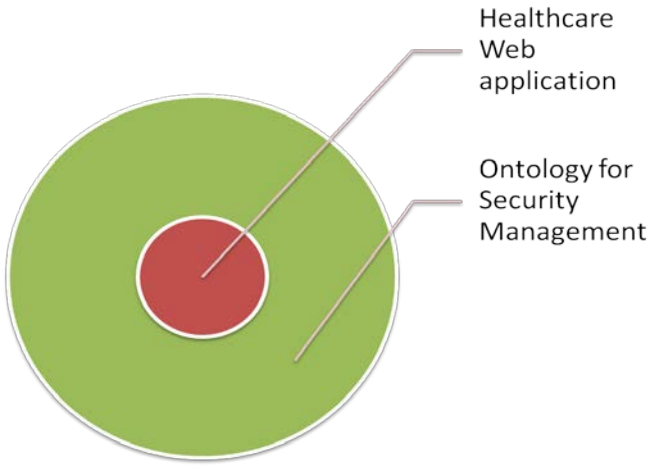

Fig. 2. Adopted Ontology Concept.

Fig. 2 illustrates the adopted concept for effective security measures in healthcare web application security. The core part of the figure represents the healthcare web application and its development and the outer layer of the figure portrays the ontology-based security management methodology that is going to be implemented on the healthcare web application development. Another issue that causes problems during development is the extensive and huge amount of information available on various online and offline resources that are adopted and used by developers during development steps to make their work easier. But did not identify that these adopting concepts are perfectly developed for their field or not. Development is a phase that demands only specific customized steps and utilities developed specifically for relevant processes; any other approach or utility can cause issues. Hence, the adopted concept for developing a more effective and secure model in healthcare web applications development is facilitated effectively by the proposed model in the article. The developed model based on this approach is discussed in the next section.

Moreover, the adopted methodology works on a conceptual ideology that tells about combining ontology-based security management with the classical widely adopted development phases for making it more systematic and secure without moving to a secure development process. There are various secure development ideologies available that are complex and very costly in implementation for organizations. In this type of situation, the proposed model by adopted ideology can produce some effective and good results and portray normal security managed overview of the healthcare web application.

III. Proposed Model

Modeling a systematic conceptual model for healthcare web application development by associating an ontology-based approach is a challenging task. There are various development guidelines and best practices are available but still it is hard for developers and designers to adopt them specifically for their development scenario [16]. This type of condition was created just because of the complexity and quick demand for applications in healthcare. The competitive market of web application development creates a challenging and risky culture of quick releasing in web application development. Business always tries to release their product or software quickly and this situation creates negligence in various fundamental aspects of designing.

Further, to tackle these situations in healthcare and provide them a systematic basic security model it is very important and necessary to portray the ontology ideology of concept development. Developing a concept before totally addressing it is the basic demand of any new approach. Concept-based models as proposed in this paper open a door for researchers to attain new ideas and develop their own by associating existing. In order to do this in the proposed article, we provide a classical development step-based model with ontology-based security management which is unique on its own.

Therefore, Fig. 3 portrays a five-step combined systematic model of healthcare web application development that associates classical development steps and ontology-based security management functionality. The proposed model associates idea initiation to facilitate the phase of the web application with a blend of ontology-based security management. The conversation is something that can be referred to as comparative analysis in cybernetics [17] and managing the security always demands conversation in-between outcome and previous steps.

By focusing on this concept, a model is created that comparatively analyzes the requirement, design, and required the desired outcome of the developer to the same platform for producing effective results. The proposed model in this paper has five steps as Idea Understanding; Requirement Identification; Design & Code; Classification of Potential Possible Threads; Facilitate. All these steps are treated as classical none extra specific steps that demand extra from the developer or business.

As described and displayed in Fig. 3 the model has five fundamental steps for healthcare web application development. These steps work systematically one by one. We try to make it simple and non-complex because complexity is something that creates confusion as well as develops a lack of interest from the developer's side for the development process. Further, it is very important to understand the step-by-step working process of the proposed model that is described in the next heading of this paper.

A. Working Process of Proposed Model

A brief description of every step in the proposed model is described and discussed below.

a) Idea understanding: It is a step that initiates ideas about development. In this phase, the developer, coder, and owner of the web application discuss functionality and ideas about how the web application is going to be after development and what kind of functions the owner demands.

b) Requirement identification: After discussing and analyzing the idea of a web application it is necessary to identify which type of process, utilities, and qualities need attention during the development and design of the application. The requirement identification phase associates these demands and prepares a proper concept of relevant development for the systematic development of the application.

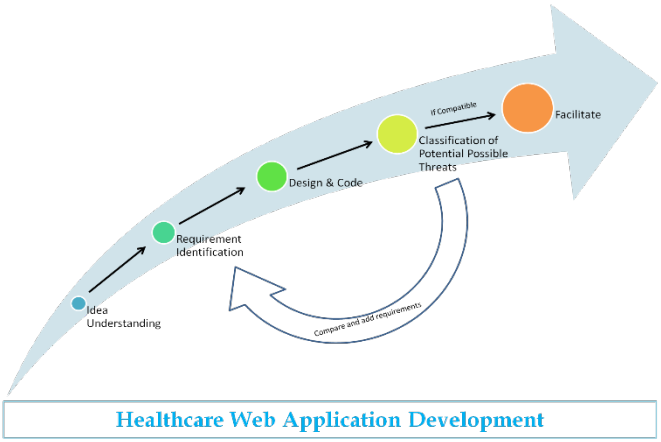

Fig. 3. Proposed Ontology-based Security Assured Model.

c) Design and Code: This is a step where developers design and code the application by associating identified requirements and prepare a systematic application according to them.

d) Classification of Potential Possible Threats: This is a step that is responsible for prevention from exploits in the system. It is a step that analyzes three perspectives and then compares the current development scenario. If the scenario was compatible according to the demand, then it's okay otherwise it again starts the loop from the requirement identification process. The whole phase description and internal working process are displayed in the following Fig. 4.

e) Facilitate: After comparing and classifying various threats and other issues of development when the whole cycle gets systematic without any interruption the proposed model allows developers to facilitate the developed healthcare web application in the industry.

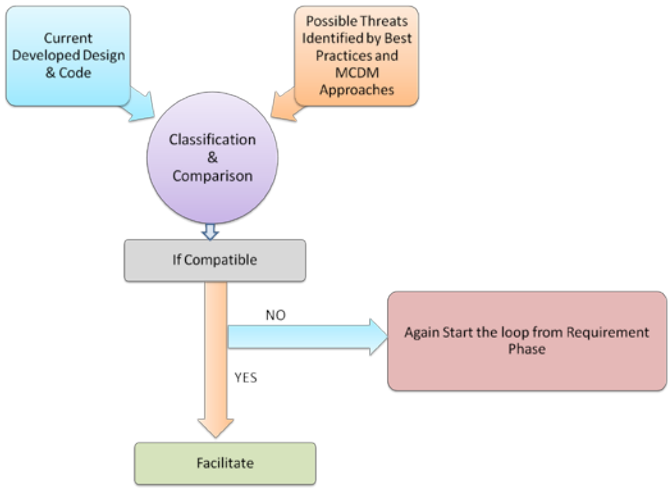

Fig. 4. Classification Phase of Proposed Model.

All in all, after discussing the concept, model, and working flow it is clear that the described model is the first initial step to facilitate healthcare web application development through an ontology-based approach. The proposed model portrays only the conceptual modeling of the idea and requires proper mathematical experimentation and validation in the future.

IV. Discussion

The current healthcare digitization process demands various advanced requirements and utilities [18]. At the same time, increased attack vectors and processes created a situation where every type of post-developed prevention mechanism for breach attacks in healthcare gets destroyed by attackers. Now to tackle these situations experts and researchers believe that pre-security measures during the fundamental development phases can play a key role in healthcare security. Therefore, to facilitate this idea, and believe the authors of the proposed articles portray a conceptual model of healthcare systematic development by attaining a focus on security factor from the ontology-based approach.

V. Conclusion

In this rapid era of digitization healthcare services demand a new, novel, and fast development approach with a blend of security measures. To achieve this desired goal, we find that it is challenging and brainstorming work for them to facilitate the security measures after the development of healthcare web applications. Therefore, they think from different perspectives and manage the goal by applying ontology ideas and development phases at the same platform. This type of combination gives exclusive power to the authors about discussing and managing systematic development and security both at the same time for healthcare web applications. The proposed article portrays a model for ontology-based secure healthcare web application development. The proposed model has five simple but effective phases which aim to give a systematic secure development pathway to the healthcare web application developers. The proposed model has various beneficial advantages for healthcare web application security and portrays a pathway for future researchers to facilitate systematic development.

Acknowledgment

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references).*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] IBM.Available online:https://www.ibm.com/security/data-breach (November, 2020).

[9] HIPAA Journal. Available online:https://www.hipaajournal.com/ december-2019-healthcare-data-breach-report/ (November, 2020).

[10] HIPAA Journal. Available online: https://www.hipaajournal.com/largest -healthcare-data-breaches-of-2016-8631/ (November, 2020).

[11] Alenezi, M., 2020. Ontology-Based Context-Sensitive Software Security Knowledge Management Modeling. International Journal of Electrical and Computer Engineering (IJECE), 10(6), pp.6507-6520.

[12] Kumar, R., Alenezi, M., Ansari, M.T.J., Gupta, B.K., Agrawal, A. and Khan, R.A., 2020. Evaluating the impact of malware analysis techniques for securing Web applications through a decision-making framework under fuzzy environment. Int. J. Intell. Eng. Syst., 13(6), pp.94-109.

[13] Zarour, M., Ansari, M.T.J., Alenezi, M., Sarkar, A.K., Faizan, M., Agrawal, A., Kumar, R. and Khan, R.A., 2020. Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. IEEE Access, 8, pp.157959-157973. Bishop, M. "A Clinic for 'Secure' Programming." IEEE Security & Privacy 8.2 (2010).

[14] Alenezi, M., Basit, H.A., Khan, F.I. and Beg, M.A., 2020. A Comparison Study of Available Sofware Security Ontologies. In Proceedings of the Evaluation and Assessment in Software Engineering (pp. 499-504). R. Kumar, A. Agrawal, and R. A. Khan, (2020), A wakeup Call to Data Integrity Invulnerability, Computer Fraud & Security, Volume 2020, Issue 4, pp. 14-19. Elsevier. Available at Thomson Reuters. DOI: https://doi.org/10.1016/S1361-3723(20)30042-7.

[15] Dubberly, H., & Pangaro, P. (2019). Cybernetics and design: Conversations for action. In Design Cybernetics (pp. 85-99). Springer, Cham.

[16] Javed, Y., Arian, Q. A., & Alenezi, M. (2021). SecurityGuard: An Automated Secure Coding Framework. In Intelligent Technologies and Applications: Third International Conference, INTAP 2020, Grimstad, Norway, September 28–30, 2020, Revised Selected Papers 3 (pp. 303-310). Springer International Publishing.

[17] Grinin, L., & Grinin, A. (2020). The cybernetic revolution and the future of technologies. In The 21st Century Singularity and Global Futures (pp. 377-396). Springer, Cham.

[18] Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. Healthcare Technology Letters, 8(3), 66.