Data Security in Pharmaceuticals and Healthcare: Analysis of necessary Web Application Security Tools.

PAVAN PARDESHI

STUDENT ID: 10380700

Dissertation submitted in partial fulfilment of the requirement for the degree of Masters in Business Administration Cloud Computing at Dublin Business School

**Supervisor: Tom Wall**

**January 2020**

# 

# DECLARATION

I declare that this dissertation that I have submitted to Dublin Business School for the award of MBA Cloud Computing is the result of my own investigations, except where otherwise stated, where it is clearly acknowledged by references. Furthermore, this work has not been submitted for any other degree.

Signed: Pavan R Pardeshi

Dublin Business School

Student Number: 10380700

Date: 6th January 2020.

# ACKNOWLEDGEMENT

I would like to thank my course coordinator and supervisor Mr Tom Wall for guiding me and helping me throughout my MBA Dissertation coursework. They helped to understand and adapt to the new system in Dublin Business School. I am grateful that I have got an opportunity to study and be a part of DBS. This year in Ireland has moulded me as a new person and now I look forward to the new opportunities. Last but not the least I want to thank all my classmates for being extremely supporting and inspiring and including me in a country and university.

# ABSTRACT

This research was conducted to identify the importance of application security testing tools which are being used in the pharmaceutical and healthcare industries. The aim of this research is to invent a new idea of integration or combination of application security testing tools to minimise the risk of a data breach. The study generated by this research was carried out by using qualitative analysis and the philosophy used was interpretivism. Here, the data collection method has been done by conducting interviews of experienced staff of application security testing department of IT companies who are providing application support for healthcare and pharmaceutical industries. Collected data then analysed by the inductive approach in which the data first has been observed, then it has been summarised with the help of Nvivo tool to generate a pattern. Accordingly, on the basis of this pattern, an invention of theory taken place. The participants for the interview were selected on the judgemental basis and 9 interviews were conducted.

The results of this research states that not every application security testing tool is fully reliable and perfect for the system. Hence, to reduce the risk of data loss and data breach, integration of two or more tools can be developed which are based on the SAST, DAST, IAST and RASP techniques. Also, the organizations are facing cost or budget issues while selecting the right tool for their work environment and end up with compromising security. Human errors are also evenly responsible for the data breaches happening in recent years. Therefore, to reduce the errors, strict policies should be adopted by the organizations and mandatory training have to arrange for the staff.

Furthermore, this research recommends that the organizations should implement the security awareness camps and train the staff actively every month and improve the policies. In addition to this, pharmaceutical and healthcare organizations should use hybrid models of the application security testing tools to avoid the data breach. Developers should also work on the integration of two or more trending tools such as Apptrana and Wireshark by taking cost, legislation and system compatibility into consideration for small scale as well as MNC’s over the world.

Table of Contents

[DECLARATION 1](#_Toc29235200)

[ACKNOWLEDGEMENT 2](#_Toc29235201)

[ABSTRACT 3](#_Toc29235202)

[1 INTRODUCTION 7](#_Toc29235203)

[2 LITERATURE REVIEW 11](#_Toc29235204)

[*2.1 Literature Introduction* 11](#_Toc29235205)

[*2.2 Literature theme one* 13](#_Toc29235206)

[*2.3 Literature theme two* 24](#_Toc29235207)

[*2.4 Related Work* 28](#_Toc29235208)

[*2.5 Literature Conclusion* 31](#_Toc29235209)

[3 RESEARCH QUESTIONS 32](#_Toc29235210)

[4 METHODOLOGY: 34](#_Toc29235211)

[*4.1 Methodology Introduction* 34](#_Toc29235212)

[*4.2 Research Design* 36](#_Toc29235213)

[4.2.1 Research Philosophy: 36](#_Toc29235214)

[4.2.2 Research Approach: 37](#_Toc29235215)

[4.2.3 Research Strategy 37](#_Toc29235216)

[*4.3 Sampling - Selecting Respondents* 38](#_Toc29235217)

[*4.4 Data Collection* 39](#_Toc29235218)

[*4.5 Data Analysis* 41](#_Toc29235219)

[*4.6 Research Ethics* 41](#_Toc29235220)

[*4.7 Limitations of Methodology* 42](#_Toc29235221)

[5. DATA ANALYSIS: 44](#_Toc29235222)

[6 FINDINGS BASED ON INTERVIEWS AND DISCUSSION: 50](#_Toc29235223)

[*6.1 Analysis of Vulnerability Scanning Tools:* 67](#_Toc29235224)

[*6.2* *Summary of Interviews:* 69](#_Toc29235225)

[7 CONCLUSION AND RECOMMENDATIONS: 69](#_Toc29235226)

[*7.1 Further Recommendations:* 71](#_Toc29235227)

[Works Cited 74](#_Toc29235228)

**List of Tables:**

[Table 1 Wireshark Advantages and Disadvantages 39](#_Toc29231676)

[Table 2 Apptrana Advantages and Disadvantages 39](#_Toc29231677)

[Table 3 Acunetix WVS Advantages and Disadvantages 40](#_Toc29231678)

[Table 4 Amazon Cloud Front Advantages and Disadvantages 40](#_Toc29231679)

[Table 5 Imperva Cloud Application Security Advantages and Disadvantages 40](#_Toc29231680)

**Tables:**

[Figure 1 10 Major security threats in Cloud Computing (securitycommunity.TCS, 2017) 7](#_Toc29231156)

[Figure 2 GROWTH OF WEB APIS SINCE 2005 9](#_Toc29231157)

[Figure 3 HOW API PROVIDES A SURFACE FOR ATTACKERS. 10](#_Toc29231158)

[Figure 4 SQL Injection Flow 11](#_Toc29231159)

[Figure 5 Cross-site scripting flow 11](#_Toc29231160)

[Figure 6 Use of software in Pharmacovigilance 16](#_Toc29231161)

[Figure 7 Research Onion (Tonuchi Joseph, 2019) 21](#_Toc29231162)

[Figure 8 Qualitative Analysis Process (Adu, 2016) 27](#_Toc29231163)

[Figure 9 Word Cloud 28](#_Toc29231164)

[Figure 10 Word Tree 30](#_Toc29231165)

[Figure 11 Graph of Designation of Participants 31](#_Toc29231166)

[Figure 12 Graph of tools preferences. Single tool Vs Hybrid tools 33](#_Toc29231167)

[Figure 13 Process flow of the application security testing tools 33](#_Toc29231168)

[Figure 14 Graph of ratings of testing tools 34](#_Toc29231169)

[Figure 15 Pie chart of ratio of participants observation of malicious activities due to API 37](#_Toc29231170)

[Figure 16 Attacks percentage due to API vulnerabilities as per the participants observations 38](#_Toc29231171)

# 1 INTRODUCTION

Nowadays, due to the digital economy, the dependency of IT systems on every business is rapidly increasing. On the other hand, pharmaceutical industries have spread massively across the world and moving to the cloud or working on the software and tools in their work environment.

Software or applications in the pharmaceutical industries play a major role in clinical research and in the maintenance of the clients and patients record. Secondly, it also helps to minimise the workload and administrative burden because if the data is stored and accessed by a single location then one can consolidate and research at the same time for clinical trials. Organizations use these softwares because it allows individuals to enhance the speed and it also increases the efficiency of the work such as to manage the records of patients, to analyse their previous records for research purpose, to make plans accordingly and at the end for performing and reporting the data. (M, 2018)

Pharmacovigilance is one of the departments in the pharmaceutical industries which use these tools to determine the safety of patient’s medication records. These healthcare industries are constantly under scrutiny.

Most pharmaceutical and healthcare industries use multiple IT Cloud services from different service providers for their business which is mainly known as the public cloud platform. On the other hand, they also want to keep some workload in the house as it may be private data which needs to be secured which is known as a private cloud platform. Now to manage these two outsourced cloud platforms and internal cloud platform (Hybrid Environment), major cloud platforms have to standardize their API’s which appears to be a major challenge at this stage to protect the data from unauthorized and unwanted access from the rest of the world. APIs are used to build a communication platform between systems for better interoperability. Healthcare organizations face challenges accessing and sharing data, especially as healthcare IT infrastructure migrates to the cloud, and digital information becomes an industry standard. In the systems, different data sets use different formats which make interoperability between apps and software with the base system challenging. Secondly, security is also one of the major concerns of cloud computing technology. Many incidences such as Data breaches, hacked interfaces and Apps, account hijacking, broken authentications are nowadays increasing. Therefore, Cloud Access Service Broker is one of the solutions of the new emerging category to manage service identity.

According to the World Journal of Pharmaceutical Research, Computer System Validation is the most important term which every FDA Regulated companies must follow. It is mainly because, in production, research as well as laboratories, software plays an important role to enhance the system efficiency and to document the pieces of evidence that these systems fulfil the intended purpose. This concept of Computer System Validation was invented in the 1970s by the Associate Director of Compliance at the US FDA, called Ted Byres. The Computer System Validation includes a number of analysis, audits, walkthroughs, surveys, and detectability works out. In which, Dynamic Software Testing is the part of computer system validation which requires the set of static testing activities through the SDLC. (Omprakash G. Bhusnure, 2016)

Due to the unpatched vulnerabilities, many incidences of global data breach have happened in recent years. For example, Equifax hack of 2018, according to the report of Government Accountability Office, there were 9000 queries fired on around 51 databases over a period of 76 days. This hack was to gain access to the personal information of the 145 million people from the countries such as the USA, Canada and UK. (Reading, 2018) Organizations such as Google’s Project Zero and the United States Computer Emergency Readiness Team (US-CERT), are solely working on the project of Zero-Day Vulnerabilities and other cyber activities. This includes the improvement of the application security testing activities as well as the database management to protect data from cyber-attacks. Around 60% of organizations are suffering from the data breach issues in between the year 2016 and 2017. (Worrall, 2019)

**Research Hypothesis:**

The aim of this research is to identify the current trending application security testing tools. Moreover, the qualitative analysis method has helped to seek proper information about the Advantages and Disadvantages of these tools in the work environment.

In this competitive world, instead of remediating the vulnerabilities, organizations are investing their time to manage the vulnerability patterns as well as to analyse duplicate vulnerability data. Organizations are spending more on skilled people who can handle the tools and the activities and cover the licencing fees. On the other hand, they are neglecting to set up the deceivability they need. Therefore, only the investment into the application security testing tools and the skilled employees is not the only solution to protect the organization and their database. Each tool manages and scores risk factors differently and if the organizations are using multiple tools then there might be duplication of the indicated vulnerabilities in the report. (Worrall, 2019)

Hence, in the end, it is utmost important to develop the tools which can be an integration of two or more tools. It is not the actual integration of the tools but the idea behind this is to merge the benefits of the tools which will accordingly minimise the disadvantages and reduce the risk of data loss. After the integration, developers can have a single tool which can provide the topmost features which are needed and which are developed by each integrated tool. Factors such as system compatibility, cost efficiency, filtration features, easy user interface and so on which needs to be taken into consideration while the integration.

According to the blog of synopsis editorial team, instead of using a single tool for the application security testing, use of hybrid models can be a better option for the performance improvement of the organizations. During the webinar series of Synopsis with John Steven, it has been observed that organizations have a specific or limited budget for their organizations due to which they acquire only one tool or just a firewall and dynamic testing tools according to their maximum needs. Web applications trace 20% of the vulnerabilities, on which organizations should not rely in terms of the data security. Hence, to reduce the risk of data loss, a hybrid approach of application security testing tools is one of the solutions which can protect the database effectively in the pharmaceutical industries. Additionally, benefits of manual, as well as automated testing, can be an added advantage for the organizations in terms of scalability and flexibility. (Team, 2015)

Combination of Application Security Testing Tools improves and simplifies clients experience while maintaining security and being reliable. It provides a baseline to create advanced information reporting and analytics service and reduction in fraud as well as risks by verifying applications or APIs in the run time environment, which allows organizations to intercommunicate and protect the environment quickly. However, every interface, as well as a web application, is not that secure because according to the Gartner Research report, in cloud security the APIs could be one of the reasons to hack the systems. (securitycommunity.TCS, 2017)

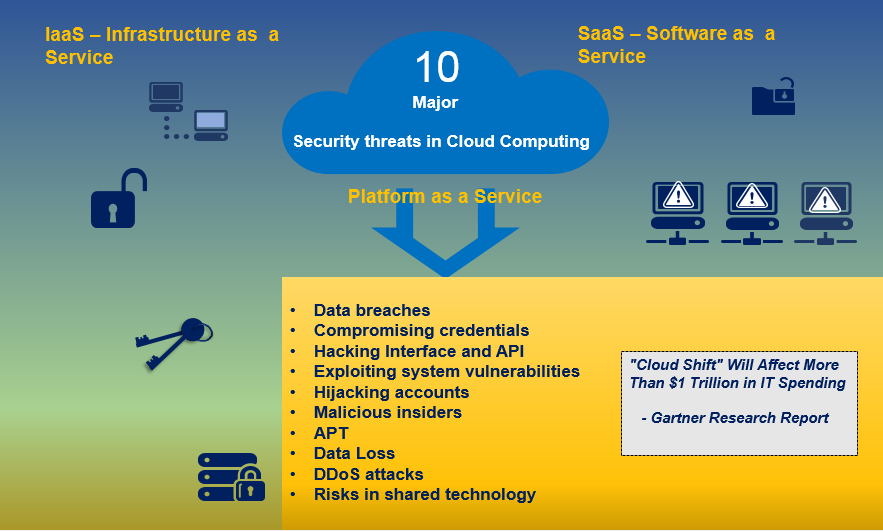


Figure 1 10 Major security threats in Cloud Computing (securitycommunity.TCS, 2017)

Here, the role of Application Security Testing Tools is to detect the vulnerability or the malicious activities running on the system network.

Hence, the aim of this research to provide a framework to reduce the security issues in the programming interface of the software used as well as to propose a brief introduction to necessary application security testing tools. This research also helps to every healthcare industry to determine the loopholes in their current systems and to maintain the records of the clients and patients safely with the help of such tools. Also, it will be more helpful for the pharmaceutical and healthcare industries to select one of the analysed tools for their organization’s database security.

# 2 LITERATURE REVIEW

## 

## *2.1 Literature Introduction*

In every business of the pharmaceutical industry, other than the development of the products and services, they need to maintain the record of such information in their work environment. Management of data is an important part of the pharmacovigilance (PV) due to the continuous generation of patient’s safety data. The information generates many modes such as clinical trials, post-marketing programs, spontaneous reports, and literature or legal reports. PV case processors collect these records, monitor, and track the serious adverse events which are the medical dose that may result into death of the patients, serious and medically significant adverse drug reactions (ADRs), and other medical-related product information. Many researchers are working on securing the web application testing and developing the tools with better safety regulations to perform these daily tasks of PV. (Ritesh Bhangale, 2017)

In the year 2017, Ransomware attack WannaCry was the major cybersecurity incident in the healthcare sector. In this US Hospitals and UK’s National Health Servis were affected. Other than this, in May 2017, Singaporean residents personal records were breached which was a potential threat to patients whose information had been revealed. Furthermore, in July UnityPoint Health became a victim of the phishing attack and lost 1.4 million records. (Pitman, 2019) Hence, the aim of this research is to provide a better solution for these industries by analysing the previous researches (which are focusing on the security of the database with the help of a combination of new technologies) and the current scenarios in the pharmaceutical and healthcare industries. However, the previous researches which are included in this paper support that the APIs and software on the cloud have to be secured to reduce the data breach risks. Researchers also stated the problems in a cloud computing environment and the need for standardization and interoperability of application security testing tools. On the other hand, few also stated the importance of information technology, healthcare data security in cloud-based applications in the pharmacovigilance, their importance and challenges which needs to be addressed from an industry perspective.

Lastly, the research objective is to provide a framework for application security testing tools which are currently in use. Also, this paper will analyse the application security tools which are widely being used in the organizations to monitor the malicious activities in their CI/CD pipelines. The applications such as Apptrana, Amazon CloudFront, Acunetix Vulnerability Scanner, Imperva Cloud Application Security, etc will be observed and analysed on the basis of their advantages as well as disadvantages. All the papers and their implementations are further divided into themes mentioned below.

## *2.2 Literature theme one*

Literature theme one starts with the report of the use of API in the organizations nowadays. According to the survey of growth in web APIs in PV since 2005 till 2018 is mentioned in the graph.

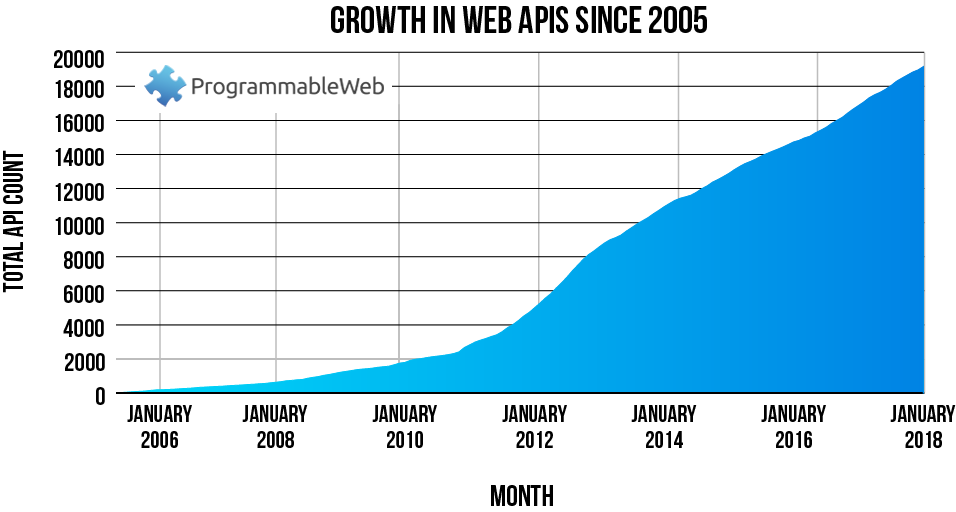


Figure 2 GROWTH OF WEB APIS SINCE 2005

Statistics show that the use of the application programming interface is rapidly increasing in every organization and the graph is increasing since 2006. During the years 2008 and 2012, it has been seen that the use of API’s is significantly increasing but from January 2012 till 2018, the huge increase in the adoption of API’s can be observed. This explains that in every business API’s plays a massive role for better performance which reduces the efforts and time of users and their workload management. API’s are a focal point of cloud innovation, exposure of data and information to the application used by front end-users in the cloud is done by API. (Santos, 2019) The interest in providing API’s is high enough to support this research in case of the importance of API in every organization. Whereas, application security testing tools, provide a way to minimising the risks of data breach in the cloud.

**1. (Tsern-Huei Lee, 2013)**

In 2013, Tsern-Huei Lee and Meng-Yu Wu conducted research based on the “Design and Implementation of Cloud API Access Control Based on OAuth”. According to the research, they explained that the cloud services can give better services through standardized API which follows a standard format in terms of safety with the help of open technologies. APIs allows developers to use existing applications developed by different developers and increase the power of their own application. Most cloud providers use their own API gateway to serve as a single-entry point into the application. As API’s are exposed via a gateway which is a single or centralised entryway into a system allowing multiple microservices to act for the users, it has become vulnerable. Hence, API technologies were designed for integration, security. In this research Tsern-Huei Lee and Meng-Yu Wu mentioned that the cloud computing security majorly depends on the management and analysis of the API’s which needs a strong API access control model. However, they also provided a well-designed API access control mechanism based on OAuth which simplifies its process flow under different application scenarios. On the other hand, the limitation for this research they observed that is the third-party applications allows to store the resource owner’s credentials (such as UID, Passwords and personal information) and gain overly broad access to the resource owner’s protected resource.(Tsern-Huei Lee, 2013)

This report will help to build an overview of the API’s security which then will be used for the analysis and framework of the overall Application security testing tools to use in the pharmaceutical industries.

**2. (white, 2014)**

According to White Paper CA technologies in September 2014, API provides the entry point into the systems for attackers to work with. This explains that the API increases attack surface easily if the security policy of application security testing tools are not taken into consideration. This can be explained better by the diagram below. Every API has its own instance, and which is unique as well as it has different risks factors based on the implementation and interface. These attacks fall under three different categories which are parameter attack, identity attack and man-in-the-middle attack. Hence, it is very important to secure your API in cloud computing to protect the organization's private data such as patients personal information as well as their medical records. (Paper, 2014)

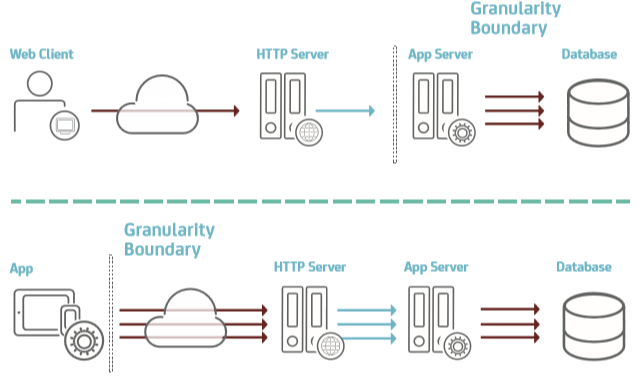


Figure 3 HOW API PROVIDES A SURFACE FOR ATTACKERS.

Other than these three categories of attacks, there are other ways which contribute to the data breaches which are SQL injections, cross-sight scripting, etc.

1. **SQL Injections:**

Figure 4 SQL Injection Flow

1. **Cross-Site scripting:**

Cross-sight scripting is the most common vulnerability observed. (Yao-Wen Huang, Securing Web Application Code by Static Analysis and Runtime Protection ) In which the attackers inject the code in the web applications code, so that if anyone tries to access the web application then an attacker can easily fetch the data from the database.

Figure 5 Cross-site scripting flow

Even though the API plays a pivotal role by providing a graphical user interface for the users in the internet of things, they remain the base for the threats while the development of applications and API because the API vulnerabilities are not that easy to track and spot. For this, the specialised tools, techniques as well as a strong framework for the security check of application is required for detection and prevention of any data breach. (Macy, 2018)

This example will help to focus more on the application side of SDLC and it can help to keep the research on the right direction towards the security of database of pharmaceutical organizations with the help of a combination of application security testing tools. This example or research paper provides the focal point which is Application programming interfaces can provide a surface for attackers and this risk can be minimised by the expected analysis of the comparison of security testing tools as well as the idea of integration of tools.

**3.** **OWASP API security top 10:**

Open web application security is the project report which is generated after every three or four years. This is a survey to detect any voids of APIs which might allow the hackers to get unauthorized access to the database. According to the report of 2019, below mentioned are the current factors which are affecting APIs or these are the trending processes by which APIs can be vulnerable and can be used as an entry point for the database access.

* Broken object-level authorization: Object-level authorization is the mechanism which validates that the users can only access the objects for which they should have access to. However, broken object-level authorization or the failure in the object authorization leads to the unauthorized access to all the database and one can alter the data easily. For example: During the network traffic monitoring process, the custom HTTP request header “X-User-Id: 54796” can be used to gain the successful HTTP response and access of other users data by replacing the value of User-Id: with some other number.
* Broken authentication: Credential stuffing is the process to gain unauthorized access to the data by using a list of valid usernames and passwords. The API which allows this credential stuffing can be vulnerable and hackers can get access if the credentials are valid.
* Excessive data exposure: The API gives access to full data objects which are stored in the backend database. Here, the applications used by clients, use the filters to disclose the data which user wants to view. However, hackers in this case directly call the API so that they get direct access to the sensitive data also that the user interfaces filter out.
* Lack of resources & rate-limiting: The API can be a vulnerability if one of the factors is missing or set up improperly.

Immoderate timeouts, maximum allocable memory, running processes limit, uploading size, amount of requests coming from each client or resource and the number of records returned from a single query.

These terms should be taken into consideration to avoid API vulnerability as the API consumes the resources such as CPU, network, memory as well as storage.

* Broken function level authentication: The APIs contain an endpoint which should have access to admin only. This endpoint is - GET /api/admin/v1/users/all and contains all the user information­ of the application. However, it does not require any functional level authorization-checks. In such cases, hackers can learn the structure of the API and manage to gain unauthorized access to this endpoint which then disclose the sensitive information of the users.
* Mass assignment: This mass assignment can be explained by the example of ride-sharing application, which includes the details of the user and one can edit the basic information of their profile such as user\_name, age, credit\_balance etc for which the API call is sent to PUT /api/v1/users/me.

The request GET also includes the credit\_balance object with the values such as:

{"user\_name":"inons","age":24,"credit\_balance":10}

Attackers can change or replays the request with the values such as:

{"user\_name":"Any","age":61,"credit\_balance":999999}.

As a result, hackers get the credits without paying for it because of the vulnerable endpoint by the mass assignment.

* Security misconfiguration: The reasons behind the vulnerability of the API might be the security misconfigurations. This is due to the missing security patches; Unnecessary enabled features, missing TLS, missing policies and improper policies. Attackers can find the .bash\_history file of the root user and can use the commands fired by the DevOps team to access the API. For example,

$ curl -X GET 'https://api.server/endpoint/' -H 'authorization: Basic Zm9vOmJhcg=='

An attacker can also find the new endpoints which are used by the DevOps team and use the information for their profit.

* Injection: In an application with basic CRUD functionality for operations with bookings, attackers can identify that the NoSQL injections can be used to delete the booking requests made by users through bookingId Query string parameter. Here, to delete the bookings, request looks like,

DELETE /api/bookings?bookingId=678 and the function which is used by the API server is as follows:

router.delete('/bookings', async function (req, res, next) {

try {

const deletedBooking = await Bookings.findOneAndRemove({\_id' : req.query.bookingId}); res.status(200);

} catch (err) {

res.status(400).json({

error: 'Unexpected error occured while processing a request'

});

}

});

Furthermore, an attacker changes the request by modifying the query string to:

DELETE /api/bookings?bookingId[$ne]=678 and as a result this SQL Injection deletes the other users booking information. Similarly, these injection techniques are the trending ones for reaching the database.

* Improper assets management: Report explained this factor by the example of an attack scenario due to which the API can be vulnerable. Here, improper assets management includes the no expiry plans for API versions, out-dated host inventory, missing integrated service inventories and old API versions which are running unpatched.

Report says that the scenarios of local search service, in which the previous version of API, api.someservie.com/v1, kept on running unprotected, which has access to the database. On the other hand, the latest version of the application became a target for attackers in which they found the latest API address api.someservice.com/v2. In this case, attackers gain the access to previous and unprotected API by replacing the parameter v2 by v1 in the URL due to which the PII (Personal Identifiable Information) of over 100 million users became available for attackers.

* Insufficient logging & monitoring: API is vulnerable if it does not produce any logs and insufficient logging information. Also, the log injections, unmonitored logs and unmonitored API infrastructures can also be responsible for the vulnerability.

For example, one video sharing platform was attacked by using the credential stuffing attack. Hence, failed logins were being logged in the log file and no alerts were triggered during this whole timespan of the attack. As a result, the user complained about the unknown login scenario and then the log files were analysed in which the heavy credential stuffing attack was detected. In the end, the company announced to reset the passwords of all users and to report the incident to regulatory authorities. (Project, 2019)

These examples of the attack can be considered while inventing the idea of combined web application security testing tools. If these scenarios can harm the overall database of other organizations then all the Pharmaceutical and Healthcare industries should consider these as a part of mandatory policies and take the required precautions to minimise the risk of data loss due to API vulnerability.

**4.** **A Survey of the State of Cloud Computing in Healthcare**: (Sanjay P Ahuja, 2012)

Healthcare industries are currently moving to cloud services. A survey of cloud computing in healthcare explained the benefits of cloud computing in healthcare such as improved patient quality of service collaboration between healthcare industries and IT cost reduction. Also, challenges faced by these industries, are briefly explained. Apart from the benefits, to prevent malicious activities and hacks, organizations should ensure that their service providers are following security measures of authorised organizations such as CSA (Cloud Security Alliance) who provides best practices for the secure cloud computing environment. Researchers of this paper also agree that the amount of private information which healthcare organizations handle could be used by the hackers for their profit. To reach out to this database, hackers can use the unsecured APIs by gaining unauthorised access controls and interfaces, are one of the targeted ports for the attackers and this should be taken into consideration from the point of the business aspect.

**5. Towards Healthcare Data Security in Cloud Computing:** (Huda Elmogazy, 2013)

Researchers in this paper proposed the solution for the data security by focusing on the particular cloud computing healthcare security compliance and encryption techniques with splitting key, key delegation and FHE algorithms. To propose the hypothesis, researchers referred to the top seven threats identified by CSA (Cloud Security Alliance) as follows:

* Use of cloud computing for criminal activities
* Insecure API
* Destructive insiders
* Shared technology vulnerabilities
* Data leakage
* Account highjacking and unauthorised traffic access controls
* Undefined and unknown risk profiles

This tells us different factors affecting the security in cloud computing in which the insecure application programming interfaces is also one in the top list causing malicious activities in an organization which may lead to the cybercrime. To prevent these security issues and unauthorised accesses, encryption model such as FHE(Fully Homomorphic Encryption) and centralised secure data sharing by encrypting the data to protect it from the malicious activities, writers provided a framework in this paper.

**6. e-Healthcare Cloud Computing Application Solutions: Cloud-enabling Characteristics, Challenges and Adaptations:** (Dr. W. Liu, 2013)

Researchers introduced cloud adaption framework and design for e-Healthcare cloud and networking solutions. In this research, writers also mentioned that the confidential data security issue is still trending in addition to the regulatory and resource distribution issues. Based on the observed challenges, researchers developed the framework for Architecture of Cloud Adaption and the benefits include critical health information technology adaption into a cloud environment which allows the evolution of interconnected cloud solutions for e-Healthcare applications.

**7. Cloud Computing for Improved Healthcare: Techniques, Potential and Challenges:** (Roma Chauhan, 2013)

Although there are several models of cloud computing such as SAAS, IAAS, PAAS; cloud service provider’s use these platforms to provide a better service for their clients. However, there are some challenges which include security risk for healthcare and pharmaceutical organizations. This paper mainly focused on these challenges and proposed an overview of safety issues and utility of big data mining in cloud computing for data mining in healthcare and pharmaceutical for better decision making in healthcare. In which the security risk due to interface issues are the major point of concern. (Roma Chauhan, 2013)

## *2.3 Literature theme two*

**1. Software used in pharmacovigilance and clinical trials:** (Dr Apoorva B.M)

Department of pharmacology of S.S Institute of medical science and research centre generated an article explaining the introduction of how the software is being used in the pharmacovigilance department.

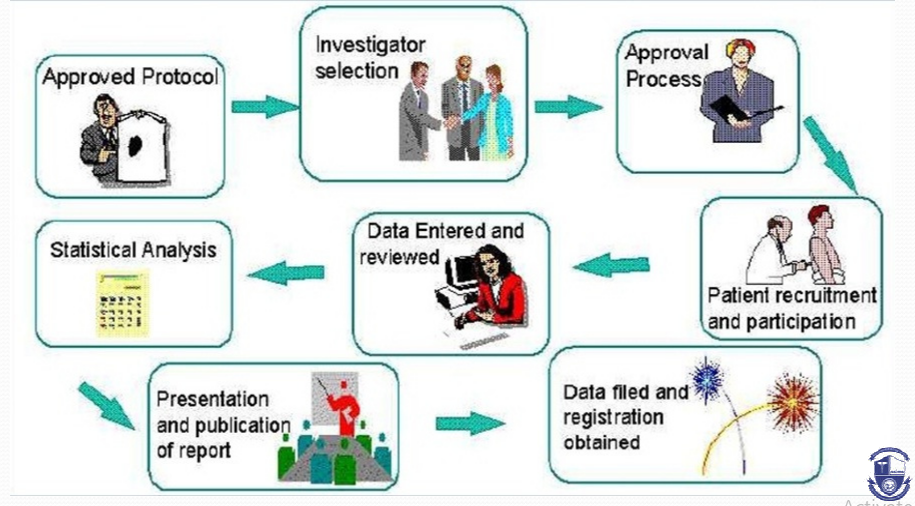


Figure 6 Use of software in Pharmacovigilance

According to the World Health Organization (WHO), Pharmacovigilance is the science and activities relating to the processes in pharmaceutical industries such as detection of adverse effects, assessments, understanding and prevention of drugs and other drug safety problems. (WHO, 2019) The image explains the process of how and where the softwares are being used. Activities such as adverse event of drugs reporting, drug reaction data management, regulatory reporting of individual case safety reporting and signal detection in adverse drug reactions are mainly performed daily in this process. However, to run these processes and reports, the major softwares which are used in this are as follows and needs to be secured so as to protect systems and database:

* ARISg:- Used for management of Adverse event reporting and adverse reactions.
* PvNET:- Used for data entry purpose, scientific assessments, data validation, cross-validation checks and MedDRA (Medical Dictionary for Regulatory Activities) version management.
* ARGUS:- Used to manage data from multiple sources and to access flexible drug safety database.
* Oracle AERS:- Analysis of adverse event reporting in for all the medical products.
* PV Works:- Used to collect report safety data to meet all common international regulation.
* Clintrace:- Used for clinical research processes and drug surveillance as well as post-marketing approval.
* PCV manager:- Data management based on medDRA industry data standards.

The tools which are used for post-marketing surveillance are as follows:

* VigiFlow:- Individual case safety report analysis is done by using this tool.
* VigiLyze:- Used to monitor international patients safety data such as medical reports.
* VigiBase:- Used to oversee Information about the security profile of medications and aggressive items and streamline inquiries.
* PaniFlow:- Used to observe alternative dispute resolution during an influenza pandemic.

This article explained the importance of the above-mentioned softwares used in an organization to improve the quality of the services provided by them. Hence, with reference to this, the framework for the applications security tools has been delivered.

**2. Information technology in pharmacovigilance: Benefits, challenges, and future directions from industry perspectives:-** (Lu, 2009)

The report of “Information technology in pharmacovigilance: Benefits, challenges, and future directions from industry perspectives” by Zhengwu Lu explained the development and use of standard-based pharmacovigilance system. This is possible by integration of connection with the e-clinical records and medical data. Clinical data management system serves as an aid to enable precautions in drug safety, data mining, result elucidation, clinical collaborations amongst various stakeholders and respective functional groups. Accessible global safety database is the database containing Adverse Events, Serious Adverse Events, Serious Adverse Drug Reactions and pregnancy reports for the Combined Therapy, and will be the legitimate information hotspot for administrative announcing and reacting to administrative questions as for the Combined Therapy Clinical Trial. Updating this database will be beneficial to enhance the detection, maintenance and communication in clinical data and relative safety concerns. Owing to the recent high-profile drug safety data challenges and problems, the pharmaceutical companies and healthcare industries have to encounter enormous regulatory obligations and enforcement with increased accountability demands to safeguard the sensitive data and welfare of patients. The pharma industries are evolving enormously. Due to this changing scenario, a proactive approach in dealing with drug safety and pharmacovigilance is the prerequisite for the biopharma industries today.

Considering these challenges in the pharma industry, research will now be focusing on the problems in pharmacovigilance as well as how secured tools can reduce these issues will be analysed.

**3. A hybrid model of Internet of Things and cloud computing to manage big data in health services applications:-** (Mohamed Elhoseny, 2018)

During the research of “A hybrid model of Internet of Things and cloud computing to manage big data in health services applications” analyst observed that the time delay of medical requests such as waiting time, turnaround time of medical requests and the waste of resources utilization can be avoided if an effective mechanism is used to manage the data in a cloud environment. Hence, according to this research, analysts proposed a new model which optimise the virtual machine selection in cloud-based applications in healthcare services to efficiently manage a large amount of data in the industries where integrated. In this research, researchers divided the cloud IoT into four components such as stakeholders’ devices, stakeholders’ requests (tasks for PV), cloud broker and network administrator. Then for the VMs selection, they used three different well-known optimizers (Genetic Algorithm (GA), Particle swarm optimizer (PSO) and Parallel Particle swarm optimization (PPSO) and proposed a model on which organizations can select the better VMs for their environment. To calculate the execution time of stakeholders’ requests, CPU utilization, turn-around time and waiting time observation has been done.

The VMs selection model and standardization will be then used for developing and integrating the better cybersecurity models in the pharma industries to protect the data. Elhonseny’s report will help to manage the safe environment of the tools used in the organizations.

## *2.4 Related Work*

**1. Securing Web Application Code by Static Analysis and Runtime Protection:-** (Yao-Wen Huang, Securing Web Application Code by Static Analysis and Runtime Protection , 2004)

In this project, researchers proposed a hybrid web application security tool WebSSARI (Web Application Security by Static Analysis and Runtime Inspection) with the help of static and runtime features to ensure web application security. This tool verifies the currently running web application code with no extra annotation efforts. Furthermore, it also detects and secures the vulnerable parts of the code by automatically inserting runtime guards in the absence of programming intervention. Researchers implemented a framework of WebSSARI system which work as an extension to the existing language systems. This has been developed for the widely used web application programming language PHP. This experiment is done by verifying 230 open source web application projects on SourceForge.net and results stated that the widely used 69 projects contained vulnerabilities. Also, their contexts showed that the static analysis diminished runtime overhead by 98.4%.

**2. SANER: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications:-** (Davide Balzarotti, 2008)

SANER is the tool which is developed by combining static and dynamic techniques to detect faulty procedures in the source codes which can be tackled by the attackers to get access to the system. In this, the approach of combining two techniques in one tool is implemented by applying it to the real-world applications and the results explained that the SANER can detect a plethora of vulnerabilities due to incomplete or incorrect cleanup processes. This paper contributes to introduce a dynamic analysis technique in which the system automatically detects the code that is responsible for the errors or vulnerabilities in the code. Also, it reconstructs the code to avoid malicious activities. The source code of this tool then executes on malicious inputs to identify the faulty cleanup processes. In more technical words, the aim behind SANER is to detect XSS as well as SQL injection vulnerabilities in the applications which are being used in the organizations. At the end type based validation procedures, became limitations for this project as different scripting languages use different values of variables according to the application. As a result, these difficulties might lead to undetected vulnerabilities in the code.

**3. SAFELI** – **SQL Injection Scanner Using Symbolic Execution:-** (Xiang Fu K. Q.)

Researchers in this paper worked on the framework of the set of tool which is known as SAFELI by focusing on the problems of this toolset. SAFELI is used for detecting SQL Injection vulnerabilities in web applications. It works on Java web applications however, it utilizes symbolic execution which monitors the security vulnerabilities statistically. In the web application code, every part of the code where SQL queries get submitted, it generates one equation to analyse the detect the initial value of web controls that can be a reason for database security breach. This framework gives information about SAFELI and its components. These components are the base of SAFELI for testing purpose of the web application security. SAFELI is the tool stands for Static Analysis Framework for discovering SQL Injections. Components are as follows:

**Java Symbolic Execution Engine:** It can inspect Java Servlets, for example, the SQL inquiry area and a library of pre-set assault designs are counselled, in light of which a crossbreed string constraint is developed and sent to constraint solver for producing vulnerability proofs.

**Library of Attack Pattern:**  It is a library which contains the pre-set attack patterns which consist of SQL syntax of before and after attacks.

**Hybrid String Solver:** It helps to solve string constraint by creating valuations of factors that fulfil the constraints.

**Test Case Replayer (APOGEE):** Identifies and generates the error trace step by step once the vulnerabilities are verified.

Researchers found that the tool lies in its satisfiability approximation procedure for string constraints and hence they focused on the open problems to solve the string constraints.

**4. SUSHI Constraint Solver:** (Xiang Fu C.-C. L.)

This paper explained a constraint solver named as SUSHI. Researchers focused on the string equation problems known as SlSE (Simple Linear String Equation) and explained that this can be solved by the automata-based approach to reduce false positives of a string analysis. In this experiment, researchers implemented SUSHI constraint solver to analyse the security risks of many small web applications and in the results, this worked effectively in practice. Furthermore, it has been integrated with the symbolic execution engines to automate vulnerability investigation. The future idea which researchers noticed are to expand the constraint solver in such a way that it can consider context-free components as well as the incorporation of temporal logic operators. This research aims to safeguard web applications and the database of organizations.

## *2.5 Literature Conclusion*

In conclusion, it has been observed that the literature is based and divided into two parts. First part of the literature shows the review of data safety and security, what are the new techniques to develop the standard environment of the Applications and VMs used. The models stated in the theme one and two will then be used in current research and which will be helpful for the development of a basic framework or architecture or comparison of application security testing tools. With the help of theme number two, the current situations, the problems faced by the pharma industries will be observed. Also, the current web applications security testing tools, as well as the software used in pharmacovigilance in the pharma industries, are the point of focus in this theme. According to the researches mentioned in theme two, it is cleared that the pharmacovigilance uses much different software and cloud environment to increase the performance of the organization in their work environment. Combination of these two themes will give the overall idea about the problems and how it can be tackled. Furthermore, the comparison of the application security testing tool will be analysed to frame a recommendation to minimise the data security breach risks. The aim of this research is to propose a framework for the application security tools used and their comparison in industries which will reduce the security issue in the pharma industries. Management and maintenance of applications with the help of application security tools in a multi-cloud environment is one of the keys to secure cloud data.

# RESEARCH QUESTIONS

* Question 1:
  + Can integration of top-rated Application security testing tools make a difference when it comes to data security?
    - Question Motivation:

This question seeks to understand the overview or the idea behind the use of application security tools and the integration of the application security tools for the improvement of security solutions of the applications. The motive behind this question is to find out if the integration of these tools can reduce the risk of data breaches in the pharmaceutical and healthcare industries.

* Question 2:
  + What are the current issues companies are facing due to Application Programming Interface as well as web application Vulnerabilities which leads to the data breach?
    - Question Motivation:

The reason behind this question is to find out the current trending issues companies are facing due to Application Interface vulnerabilities. As the applications used in the environment of the healthcare and pharmaceutical organizations can be used as a gateway for hacking the database.

* Question 3:
  + How these integrated tools will help to minimise the risk of data loss and to protect the pharmaceutical as well as healthcare industries from the attacks such as Ransomware? What are their advantages and disadvantages?
    - Question Motivation:

Not every security testing tool is perfect, hence instead of using multiple tools, integration of two tools will be the future idea to improve the quality of security testing tools. Here, in this case, this question aims to find out the benefits of different tools and their weaknesses by which the comparison of the tools taken place to finalise the exact tools to integrate for the future work. This comparison of advantages and disadvantages will also be helpful for the organizations who are facing difficulties while selecting the perfect application security testing tool for their organization to overcome the security challenges.

# METHODOLOGY:

Primary aim of this research method is to collect the data from the IT department of pharmaceutical industries or the IT companies who are supporting the cloud services for pharmaceutical industries. This has been done by the qualitative analysis process in which 9 interviews were conducted. To collect these samples, the main focus was on the pharmaceutical industries and the department which will be focused on is pharmacovigilance as well as IT. The reason behind the selection of these was, software and cloud services are mainly used in this department. However, the companies have been finalised on the judgmental method which means that the research not only focuses on a single organization and their employees but also from multiple pharmaceutical companies present worldwide.

## *4.1 Methodology Introduction*

Primary research of the current title has the aim to find and invent the new ideas of integration of the application security testing tools used in pharmaceutical industries for the performance improvement as well as to reduce the risk of data breaches. To achieve this aim, a qualitative analysis technique has been taken into consideration because this research is not based on statistical analysis. The data then collected by conducting interviews of 9 employees of healthcare and pharmaceutical industries. However, for the better results, open-ended and explanatory questions were asked to the interviewees. In the end, result focus on the analysis of current trending application security testing tools used which prevents vulnerability or the malicious activities in the work environment of Pharmaceutical and Healthcare industries.

The research methodology which has been used during this research was carried out with the help of “Research Onion”. In this model, research methodologies are explained and compared. Accordingly, the selection of methods has been taken place. To provide an effective methodology, the suitable research philosophy, approach, strategy, design and ethics were used.

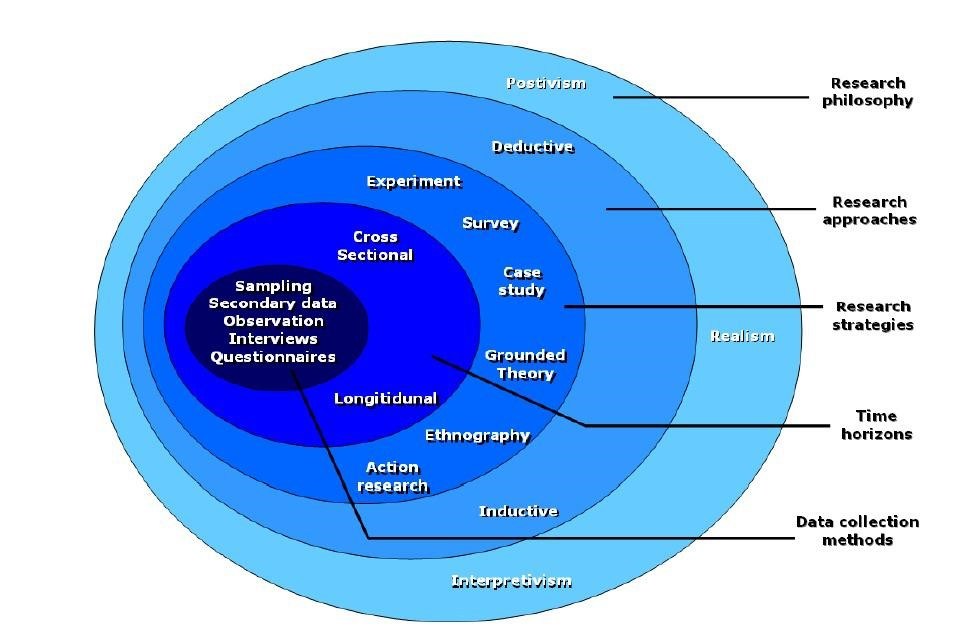


Figure 7 Research Onion (Tonuchi Joseph, 2019)

The research was designed on the interpretivism philosophy and the approach was inductive as the data first need to observe and then accordingly pattern and framework has been developed. Sample size for the research has been determined on the basis of non-probability sampling method in which the participants were selected on the judgmental or purposive sampling method. The collection of samples were divided into two groups of six participants to retrieve the exact information and the solutions on the problems such as data breach due to API vulnerabilities or insufficient tools of application security testing. Prior to the investigation, the consent form was provided to the interviewees to give a brief idea about the research and hypothesis.

The research has some limitations such as lack of real-time work environment to apply the framework or idea of the integration of applications for better results and there are other researchers working on security and safety of cloud computing which can provide a different path or applications for the overall benefits of organizations. Additionally, there are few service providers are already in the market such as MuleSoft, Microsoft Azure, AWS, Google Cloud, which provides multiple services for the cloud applications users. The limitation of this research also includes the candidates selected for the interviews. The information has been fetched from only the candidates of IT department because of the technicality of the questions and topic, whereas the front end or non-technical users were unable to explain the technical terms or tools which are necessary for the application's security.

## *4.2 Research Design*

Stepwise design of this research is as below:

* Research philosophy: Interpretivism philosophy.
* Research approach: Inductive approach.
* Research strategy: Qualitative
* Sampling method: Judgmental or purposive sampling method.
* Data collection: Face to face to telephonic or online email-based interviews.
* Data Analysis: Theme based on dividing the data into two groups of people from two different departments.
* Results: will be in the form of transcripts and statistical information.

### 4.2.1 Research Philosophy:

To finalise the right research philosophy from different types, the detailed analysis of all the philosophies has been done. However, the philosophy used in this research is interpretivism. According to the book written by (Collins, 2010), interpretivism is used to group together different approaches. The basic reason behind the selection of this process was the approach which includes comparative advantage of data validation and level of acceptance.

### 4.2.2 Research Approach:

For this particular research, inductive approach has been selected. It is because the inductive approach includes an observation of the data in the initial stage. Next, depending on the observations, the pattern has been introduced to summarise it. In the last step of the inductive approach, the theory or the standard form of analysis has proposed as a result of this research. The purpose for using an inductive approach is to condense raw textual data which is in interview-based form into a brief, summary format. Furthermore, to establish clear links between the evaluation or research objectives and the summary findings derived from the raw data and to develop a framework of the underlying structure of experiences or processes that are evident in the raw data.

### 4.2.3 Research Strategy

The strategy which has been used in this research is qualitative analysis. It is because qualitative research is a type of scientific research. In general terms, scientific research consists of an investigation that:

• Seeks answers to a question.

• Systematically uses a predefined set of procedures to answer the question.

• Collects evidence.

• Produces findings that were not determined in advance.

• Produces findings that are applicable beyond the immediate boundaries of the study.

This research technique includes the above-mentioned characteristics. In addition to that, it seeks to understand a given research problem or topic from the perspectives of the employees working in a real-time environment or who face the situations every day. Qualitative research is especially effective in obtaining culturally specific information about the values and opinions of particular populations.

In this research, the research questions and the way of research is not statistical. Other than that, the research includes in-depth investigation to provide a framework or comparison and to provide innovative structure.

Due to the above-mentioned characteristics of qualitative analysis and the limited sample size, this technique has been used in the research area.

## *4.3 Sampling - Selecting Respondents*

Sample size of this research has been determined on the basis of the employees of healthcare industries and pharmaceutical industries. The sample size is based on Non-Probability sampling method.

The reason behind choosing particularly Non-Probability sampling method is, there are n number of employees in the healthcare and pharmaceutical industries and specifically in the pharmacovigilance and IT department of pharmaceutical and healthcare industries. Therefore, not all members of the population have a chance of participating in the study unlike probability sampling, where each member of the population has a known chance of being selected. Selected participants are the employees who all having in-depth knowledge and experience of the department in which they are working to fetch the best results of the issues as well as solutions mentioned in this research and hypothesis. To identify subjective judgements for the research questions, this research is more focusing on the Non-probability sampling method.

Furthermore, respondents were selected by the Judgemental or Purposive sampling method. It is because this research needs only those people who all are experts in such field for the investigation.

Accordingly, the main focus of this research is on employees of healthcare and pharmaceutical organizations, who all are working in the Pharmacovigilance and IT department.

Another reason behind this is the pharmacovigilance department includes people who are using IT tools and software for analysis of the patient’s historical and current records. However, they also have an IT department who all are the part of the administration department. By investigating these departments, research then moved on towards the analysis of issues observed from pharmacovigilance team and innovative ideas from the IT team regarding application security testing tools and API security. Lastly, the combination of the results proposed the format of the advantages and disadvantages of Application Security Testing Tools and recommendations.

## *4.4 Data Collection*

The aim of this research was to collect data from the two different departments which are Pharmacovigilance and IT department of the pharmaceutical and healthcare industries. In the first part, more focus was on the group of six people working in the pharmacovigilance department who all are working on the front end applications to analyse patients health records. It supposed to provide the understandings of the current issues they are facing on-field and what are their requirements but while actually going through the interviews it has been seen that the non-technical employees will not be suitable for the data collection method. Hence, the method then changed. On the other hand, a group of ten people working in the IT department has been interviewed and asked the questions regarding the application security testing tools used towards data security. The result of these interviews gave in-depth information about the expected solution for performance improvement of application security testing tools.

The reason behind selecting these particular people is because the pharmacovigilance team is well expert in the field of pharmaceuticals and they need to work accurately on the patient's analysis. Another reason is that software and cloud-based tools are mainly used in this particular department. Secondly, the data gathered from these people explained whether they are facing vulnerability issues because of APIs. Additionally, their requirements of the security testing tools have been analysed by the analysis of collected data. However, the IT people working in organizations provided their solutions or assumptions to improve the performance of Application Interface as well as the application security testing tools. IT staff have provided a way for this research to develop an innovative an idea of integration of two or more application security testing tools to protect APIs as well as other applications to improve the performance of pharma industries and to prevent the data from emerging issues of data breach.

While the collection of this data there was some limitations faced in terms of the availability of the employees to interview and access to the particular departments. Also, during the data collection from the pharmacovigilance department employees, it has been seen that the information was totally non-technical as the staff was not actually dealing with the database security as well as application security testing tools.

The implementation process totally depended on the availability of employees by taking research ethics into consideration. In particular, the data collection method was face to face interview, on-call interviews as per the availability of the participants.

## *4.5 Data Analysis*

As mentioned earlier, data sets have been collected and analysed by the interviews conducted of employees of the IT department who work for the pharmaceutical and healthcare industries.

The proposed solutions and the advantages, as well as disadvantages, have been fetched from the group of ten employees of the IT department of these industries. This sample then has been analysed to discover the ideas for better performance of the software and tools used in application security testing. The collected data has been then analysed with the help of a tool known as Nvivo.

After combining and analysing the data, a combination of requirements and predicted solutions has guided this dissertation to innovate comparison or chart of benefits and challenges of Application Security Testing Tools used to protect organizations from vulnerable activities. Additionally, the aim of this research was to propose a recommendation to improve the performance of Application Security Testing Tools. First codes have been developed to divide the data into multiple factors and then these codes will be then applied to the collected data using manual coding. After categorisation of data, themes have been analysed. In the end, data summarized and linked for formulation. The theme of this analysis is basically to collect the data with the help of a questionnaire to ask while interview, then the analysis of this data, a pattern has been created and on the basis of that, the theory has been written accordingly.

## *4.6 Research Ethics*

During this research and data collection process, deep information of research provided to the interviewees for a better understanding of the concept where the questions have been asked.

Taking research ethics into consideration, consent form and participation leaflet has been provided to the participants which were signed before providing the information and conducting the interview.

This research includes some personal and confidential data of participants, which has to be secured and should not be disclosed in any case. The Informed Consent Form is used to assure participants, that the person or identification data will be kept confidential and that only aggregated results will be published to obtain their permission to identify them by name or by other characteristics.

The primary communication for this research with these participants was held by the email or verbal conversation to analyse whether they are interested in this process or not. The first brief information about the purpose of the interview has been mentioned briefly at this time. Further, according to the availability of the employees, email including consent form and participation leaflet was provided. In the end, the interview questions were asked according to the availability of the participants. For this process, the expected time was of 6 weeks to collect the data from each participant. At the end of the last 6 weeks, the collected data were analysed to develop a standard solution of APIs security and Application Security Testing Tools.

The research ethics process will consider not just the nature of the assurances given to participants but also the practical steps taken in this research to honour these commitments.

## *4.7 Limitations of Methodology*

In this research, the limitations were the real-time work environment with developers to work on API security tools. There was no real-time environment to apply the analysed or proposed integration of application security tools, which was the basic limitation for this research. Only the theoretical pattern will not be effective unless and until it has been authenticated or applied in a real-time environment. Secondly, all the topics related to security are not covered so that it will be hard to get concluded in overall aspect of data security. This research aims to propose the overview of top Application Security Testing Tools, with the help of which developers can analyse which tool is suitable for their organization to minimise the risk of a data breach. During this interview process, another limitation was the non-technical staff. Because of the lack of technical experience and expertise in the testing field, it was hard to fetch the information from the non-technical staff such as the employees of pharmacovigilance. There are so many issues regarding the security of applications which are mentioned in the literature. However, this research is mainly focusing on APIs security and application security testing tool. Therefore, all the concepts of security will not be covered other than APIs. There are other cloud service providers in the market which already developed the software to manage API or they provide APIs, but the aim of this topic is to propose an overview of trending application security testing tools and their benefits.

# DATA ANALYSIS:

Data analysis is the most important part of the research process. Hence, to analyse the data, Nvivo tool has been used. This tool is time efficiency and transparent in the services which it provides for the qualitative data analysis. It has multiple features through we can code and categorise the data to fetch the accurate results. This tool also can capture mixed data and the accommodation capacity is also very large. Therefore, to analyse the huge number of data and to categorise it with the help of graphs and maps features, this tool has been used for the qualitative analysis of the interviewed data. The main features which were being used in this research were;

* Sources of data.
* Nodes: used to categorise the data into different parts.
* Coding.
* Classification of the data
* References/ cases.

(Syarifuddin Dollah, 2017)

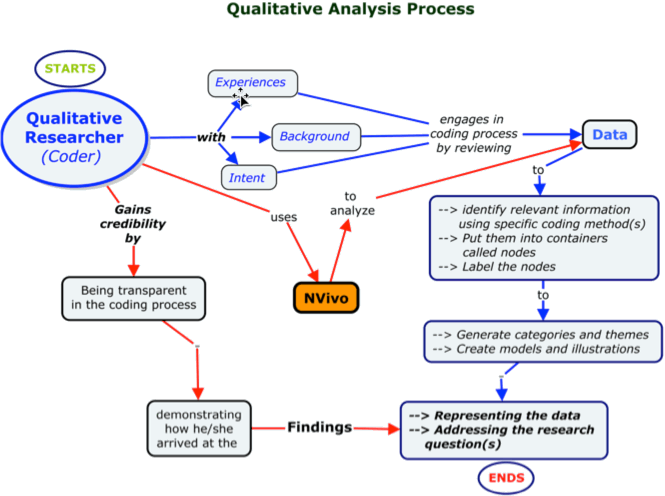


Figure 8 Qualitative Analysis Process (Adu, 2016)

Dr Philip Adu, Methodology Expert at the National Centre for Academic & Dissertation Excellence (NCADE), has explained the steps for the qualitative analysis of the interview data in brief with the help of the above-mentioned diagram. According to that the data must be transcribed and divided into the nodes. Here, nodes are the containers which contain similar data from all the interviews. In this research, the nodes have been defined on the basis of the flow of interview questions. The questions have similar objectives in which nodes helped to collect the answers into single place and divide them into the different containers such as Roles, Issues in pharmaceutical industries, Ratings of tools, Solutions to minimise the risk of data loss, Tools which are used in organizations and the workflow of the tools used in the organizations. (Adu, 2016)

The steps through which this data has been analysed are given below:

* **Step 1: Data Collection:**
  + In this step, the audio recordings were transcribed and then fetched into the database of Nvivo. After successfully uploading the data into the database, the data further has been structured as the outputs were not fitting into a common format. Hence, the interview content has been re-ordered.
* **Step 2: Disassembling**
  + In this step, after re-arranging the data, Nodes has been created and then moved and divided according to the nodes. Nodes are the containers which differentiate the data fetched from the interviews. The data then further divided with the help of the code. Code is the process in which researchers break down the information into different factors to analyse and develop new results. (Elliott, 2018)
* **Step 3: Reassembling**
  + In this step, this collected or disassembled data has been combined or assembled selectively into a group of nodes to perform tasks such as Word Cloud and Text search query.
  + Furthermore, Treemap visualization has been taken place by selecting the nodes. It shows the hierarchical data in a structure like a tree.
* **Step 4: Interpretation of data**
  + After this text search query, word cloud as well as a treemap, the deep analysis of this coded information which was generated by interviews. Results of this analysis developed a brief theory.
* **Step 5: Conclusion**
  + At the final step of this data analysis, results have been concluded by considering the real-time data received with the help of interviews.

During the data analysis, full documents analysis formed a group of words which were more likely used by the participants during the interview process. The frequently used words in the conversations are combined known as Word Cloud. Word cloud makes common themes easy to understand.



Figure 9 Word Cloud

This helped to focus more on words such as ‘Tools’, ‘Security’ and ‘Testing’ etc which are the strong reflection of the sentiments. Also, it provided the overall summary of the documents in word cloud format as a part of text analysis in the research.

Furthermore, the word tree format in this tool is used to pre-selected words and the relationship with the other words in the interview text-based data. Other than word cloud, it has been used to connect and observe the exact connection of the word ‘Tools’ in the dataset. In the result, word tree explained deeply that the importance of tools which are being used widely in the market. It has helped to analyse the dataset with respect to the tools which are being used in the market. With the help of this, the current trending tools has been observed such as Apptrana, Imperva Cloud application security, Amazon Cloudfront, Wireshark, Acunetix WVS, NetBrain, and TestRail etc.

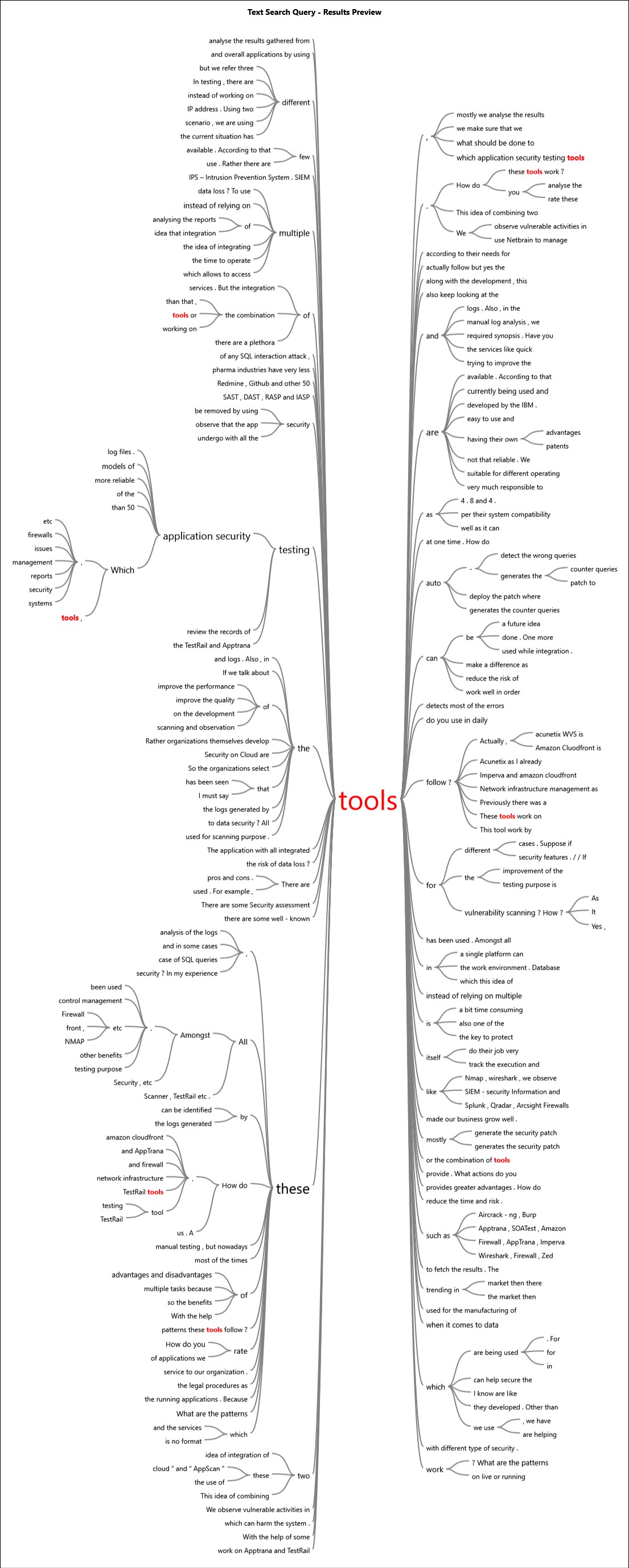


Figure 10 Word Tree

# 6 FINDINGS BASED ON INTERVIEWS AND DISCUSSION:

The interviews were conducted on the working professionals in the healthcare and pharmaceutical industries who all are working in an IT department for these organizations. The results which are observed from these interviews are explained below.

The reason behind the first question in the interview was to check whether people from which team are more likely to answer the questions which are asked in the interview. Also, to check if the people from different teams are aware of the application security testing tools and their benefits, this question has been asked. Moreover, to analyse the day to day activities of the participants in the organizations it has been asked.

**Question 1 was what are your key responsibilities in the organization?**

Where most of the participants were actually working in the security testing environment such as Penetration Tester, Administrator, Application Security Tester, Database Administrator, Security Network Engineer. On the other hand, some participants were developers and from the management field where they use to design the frameworks for clients, design the architects, arrange the audits as well as risk assessment tasks for the employees in the pharmaceutical and healthcare organization. After carefully analysing the results from all the participants, it has been observed that the information received from the participants who are working in the testing environment is more technical and brief.

Figure 11 Graph of Designation of Participants

From the graph mentioned above, it has been clear that 50% of the respondents were actually working as a Tester, 30% of the respondents were developers and the remaining 20% were from the management team. The aim of this graph is to carry out the graphical discussion of the departments of the participants. The number of testers was high as compared to the staff of the management team and development team. In the results, it has been observed that all the participants were having a good experience and expertise in the field of application security testing field from the received responses.

Moreover, by looking at the day to day activities of the participants, it has been observed that the healthcare and pharmaceutical industries are continuously working on the system as well as database security. To maintain security, it has been clearly identified that the security audits, a timely survey on systems, database backups, reviews and analysis of the records fetched from tools, risk management training for employees and lastly, analysis of security policies are the tasks which these participants or organizations follow which are currently helping them to protect the database of the organization.

Furthermore, few of the participants were developer; hence their responsibilities were to develop the applications and security. From the interviews, it has been seen that the developers are responsible for the observation of every loophole of the SDLC with the additional required security.

**Question 2 was which application security testing tools are currently being used and more reliable in pharmaceutical industries?**

This was one of the important parts of the research as the answers were directly pointing out towards the applications which are being used in the organizations and their reliability in the pharmaceutical industry. The reason why this question was asked is to see which applications are there in the market which is being used in such organizations and preferred by many. In the result of this question, every participant agreed that there are many tools available in the market and this is because of the aggressive growth of the market. Few participants stated that there are more than 50 tools available in the market and the prediction was right. According to the report of OWASP Category of vulnerability scanning tools, there are more than 53 tools are currently being listed in the report of OWASP. (OWASP, 2019) Acunetix Web Vulnerability Scanner, Apptrana, Burp Suit, App Scanner, TestRail, Jasmin, Aircrack-ng, Burp Suite, SQLmap, NetBrain, NMAP, Firewall, Wireshark, SOATest, Imperva cloud Cloud Application Security, Application Security on Cloud, Appscan, Netbrain, Cisco, Zed Attack Proxy, SIEM (Security Information and Event Management) and Solarwind, there are the application security tools which are currently being used in the market. When this question was asked to the respondents then the answer was more focusing on these tools as well-known tools in the market. Here, the reason behind asking this question was to find out the tools which are being used in the market and the response which received from all participant states that not all the tools are suitable for the systems. It depends on the type of framework as well as which operating systems are being used in the organization and accordingly by looking at the requirements of the organizations (from small scale companies to MNC), the tools were being selected for their work environment.

Participants also mentioned that all the tools have their own benefits and drawbacks; however, it has been also observed that there are different tools available in the market depending on the scenario-based attacks. Organizations maintain their records of attack scenarios for future references and for the analysis. For example Acunetix Web Vulnerability Scanner is the tool which works on the SQL Injection attacks and cross-site scripting which are mentioned in this research section 2.2. Also, to work on network security, Wireshark, Netbrain as well as Nmap are the tools which are in use nowadays.

**Question 3 was, amongst all these tools, which application security testing tools do you use in daily work routine?**

During the analysis of interview data, it has been observed that not every application security testing tool is 100% secured and reliable. Hence, organizations prefer to use multiple tools for their application security testing purpose. But, the use of multiple tools is more time-consuming. Here, according to the literature theme two (refer 2.3.3) hybrid model of the internet of things can be used to reduce the issues faced by the frontend teams. Researchers also agree with the concept that using multiple or hybrid tools can work well in terms of the challenges faced by the pharmaceutical industries (refer to 2.3.2).

While talking about the question and the data received from this, it is noted that the tools such as Wireshark, NetBrain, Apptrana, Imperva Cloud Application Security, Acunetix Web Vulnerability Scanner, and amazon cloud front are the tools which are trending in the market. One of the participants said that the one cannot rely on the use of a single tool in the organization for their database security hence; they are using more than one tool in the daily work routine to fetch the records from multiple aspects. The records of these tools can be analysed by the testers to make sure that they are not missing some vulnerable activities or errors.

Over 40% of the participants are using the single tool verification and remaining 60% of the participants believe that the multiple verifications or the use of hybrid models or use of more than one tool are beneficial to safeguard their database as well as the organization. In the end, it has been stated that the majority organizations are using multiple tools for their database security and another reason behind this is that there is lack of tools which are compatible with all the operating systems and which is the combination or integration of the multiple application security testing tools. With reference to the hypothesis of this research (refer introduction 1), it can be concluded that the use of integrated tools or hybrid model is necessary for the work environment of the pharmaceutical as well as healthcare industries. On the other hand, the reason behind the use of a single tool in the organizations was observed that majority of the organizations are facing the problems with cost efficiency and the lack of resources in organizations.

Figure 12 Graph of tools preferences. Single tool Vs Hybrid tools

**Question 4: How do these tools work? What are the patterns these tools follow?**

The IT department of healthcare and pharmaceutical industries are using tools which are already discussed above but to know the process which these tools follow is also necessary before coming to the final conclusion as well as the recommendation part of this research. The reason behind asking this question is to get familiar with the frameworks or the processes on which these tools are made. During the analysis of this question, it has been seen that these tools are following a pattern as follows:

Figure 13 Process flow of the application security testing tools

During the first step, these tools can be used for scanning the systems as well as network to detect vulnerable activities. Then developers analyse the reports generated by these tools. If the errors or suspicious activities are observed, it has been identified during research that most of the queries get resolved through the tools itself. This is because the tools are being programmed to respond and stop such activities if observed in a runtime environment for example; SQL Injection queries can be resolved with the help of these tools. However, in case of serious errors or the packages got from the frontend team, the queries then need to forward to the application security team to analyse. After the analysis, the right solution for the problem this team develop and further implement or deploy to the system. Tools such as TestRail, SIEM is the single platform which gives access to the multiple services inside these tools. With regards to that, researchers are developing the new tools with innovative ideas and features such as tools mentioned in the Related Work section 2.4. Finally, summarising all the answers received for this question, every tool has its own benefits as well as drawbacks. There are different tools available for different cases of attack scenarios. Hence, organizations are using multiple tools to scan the systems and detect vulnerabilities. Organizations are referring tools such as SIEM and TestRail to reduce the time and risk by managing test cases, tracking execution, and using the graphical representation of these tools.

**Question 5: How do you rate these tools when it comes to data security?**

Ratings of these tools are another important factor of this research by which it has been stated that every tool has its own advantages as well as disadvantages. According to the ratings and explanations on the ratings, top-rated tools have been finalised and taken into consideration for the integration purpose. Below is the graph in which the ratings have been explained clearly.

Figure 14 Graph of ratings of testing tools

Graph states that the tools which are currently being used are having the maximum ratings. But in this, few tools such as TestRail and Imperva cloud application security have been rated very less by participants. This is mainly because of the drawbacks of these applications for example; TestRail, in which to organize the work it takes too much time to understand and the user interface is can be improved. Hence, it has been rated 3.5out of 5. Another example is Imperva Cloud Application Security is the tool for which participants rated 3 out of 5 because of the application is very costly. Some small scale organizations cannot afford to spend huge cost on such tools.

On the other hand, 60% of the organizations in the retrieved data are using Apptrana, Acunetix Web Vulnerability Scanner, Nmap, Amazon Cloudfront, Wireshark, NetBrain and Firewall as their Application Security Testing Tool. According to the participants, these tools are having a very user-friendly interface as well as the tools are easy to deploy. Wireshark has a unique benefit that it can be installed on different operating systems. In the results, system compatibility is the factor which needs to be addressed while developing any application security testing tool or integrating them for additional benefits such as less time consumption, more reliability etc. Lastly, by looking at the ratings given in this section, top-rated five applications have been observed and compared their advantages as well as disadvantages in the next section of 6.1.

**Question 6: What are the current issues pharmaceutical industries are facing in terms of data security? What are your observations?**

To identify the problems or loopholes in the database security factor, every participant has mentioned that database security is one of the trending issues in the healthcare and pharmaceutical industries. Therefore, this research is aiming to detect loopholes and reduce the risk of data breach and data loss. With reference to the literature review section 2.3.2, the problems stated by the researcher are observed exactly the same during these interviews. However, it has been clearly identified that the software security or application security is still highlighted. Additionally, the reasons for these in terms of database security are lack of resources as well as the lack of software or tools which are actually required for the organizations. Lack of resource management is also one of the observed problems in the organizations which need to be addressed by the developers at the time of application security testing. One of the participants mentioned that data security is one of the trending issues in the healthcare and pharmaceutical industries and the reason behind this is tools which are being used in the organizations are not fully reliable. Testers and developers said that one cannot rely on the single tool instead, comparison of two or more reports can be more beneficial in terms of the database security.

**Question 7: Over the advantages and disadvantages of these tools, what should be done to minimise the risk of data loss?**

Besides the advantages and disadvantages of the application security testing tools, this question has been asked to the experts to find out the suggestions to minimise the risk of data loss. From the analysis of all information, it has been observed that the combination of tools which are being used in the organizations are more secured than the organizations which are relying on only one tool for security testing. Proposed solutions to reduce data loss are mentioned below. These are the actual responses and solutions which are given by the participants during the interviews.

* First of all, organizations need to make sure the data security policies are in place. Secondly, system Backup is the ultimate option for any incidents.
* Limitations of the access to users can also be helpful to prevent errors from the front end users perspective.
* Continuous scanning and observation of the tools is the key to protect the data but not every tool is reliable and fully secured, but with the help of combination of application security testing tools, the risk of data breach and loss can be reduced.
* The use of the right tool for the systems is important and to manage the resources accordingly is the key if there are limited resources available.
* The application needs to be handled in 360 degrees to protect against vulnerabilities. This can be possible by providing the integrated tool of RASP, IASP, DAST and SAST.
* To use multiple tools for the testing purpose is helpful. Apart from that defence in depth principle must be there which indicates security at each layer of the OSI model.
* Most of the times human errors cause security breach so to avoid this there should be least privileges given to individuals to avoid errors. Therefore, to provide security training with laws and regulations taking into consideration, to the employees is also one of the observed solutions which need to follow strictly.
* Idea of integration or hybrid models can be a better solution for these kinds of risks. It cannot fully remove the risk factor in the tool but it might help to decrease the risk more effectively.
* Server management and maintenance have to be taken into consideration. If the servers are not properly maintained then practically the system backup is not possible.

The summarised responses of participants and considering the literature theme one and two, the risk of a data breach can be reduced with the help of hybrid tools, reducing human errors, server management, resource management and policies improvement are the factors which have to consider to reduce the risk of data loss.

**Question 8: Can we use hybrid models of application security testing tools instead of relying on multiple tools for vulnerability scanning? How?**

The reason behind this question was to analyse the expert comments when it comes to the hypothesis of this research. As the hypothesis says that the integration of two or more tools can be an added advantage for the application security testing tools, it was the most important approach of this dissertation. Even though all the respondents were agreed to the fact of a hybrid tool, they also mentioned or suggested few tools such as SIEM, which is already being used by the developers to protect the systems from vulnerable activities. According to one of the participant's point of view, this tool SIEM provides the platform to work on multiple tasks. It is the tool which provides access to multiple tools so that one can opt into the multi-service layer platform.

On the other hand, it has been observed that the hybrid models such as integration of SAST, DAST, IAST and RASP tools will be beneficial for the organizations. In this research, it was obvious that the hybrid models can make a difference and hence, all the participants agreed that the integration is possible. However, it has also been concluded that the integration of tools based on SAST, DAST, IAST and RASP can be done but the most important factors which need to be taken into consideration are system compatibility, cost-efficiency, agility, flexibility and evolvability of the tools.

**Question 9: How do you analyse malicious activities?**

During the work environment, it has been observed that organizations which are using multiple tools for testing purpose, requires more time for the analysis but the reports are more accurate and effective in terms of security. On the other hand, organizations which are using a single tool for the application security testing, require less time but it could not be reliable.

Moreover, when it comes to the analysis of malicious activities, it has been seen that the organizations are using two types of testing manual testing and automation testing. And as the manual testing is not that secured, organizations are now using automation testing. But the developers are not dealing with these activities and they pass these queries to support team.

Other than this, testing applications are being used for manual log analysis, to trace the errors and vulnerable activities. NetBrain, Nmap and Wireshark are the tools which are then used for the network analysis. In this process, it has been seen that during the initial stage of data analysis, testers used to check the logs as well as reports which are generated by these tools. Manual analysis of logs also helps to identify the vulnerabilities in the applications. The tools in most of the cases generate the counter queries to resolve the issues identified in the scanning process but in case of the serious issues, testers which are working in support team generate the ticket for the application security team and further the security team analyse the logs, develop the security patch and deploy it in the required location.

Network security engineers in the interview mentioned that they generally use IBS and it is the most important tool in their work environment. Further, they work on CRM tools such as Splunk to reach towards the root end or in-depth of the issue occurred. With the help of these two tools, it is possible for them to analyse the bugs in source code and mitigate that end. In the end, the processes such as blocking ports, killing the running processes which are causing trouble and checkpoints are being used to resolve the issues.

The reason behind asking this question was to analyse the process and pattern these organizations follow in terms of data security. Therefore, according to the results it has been observed that the use of multiple tools to analyse the activities is the process which few organizations follow and remaining focused on log testing.

**Question 10: What actions do you take against these malicious activities to minimise the risk of a data breach?**

When asked the employees of healthcare and pharmaceutical industries, it has been observed that after the attack scenario of Ransomware, organizations are working hard on the database security. Due to which, organizations are taking all the necessary action against these attacks and take precautions from every aspect.

To fetch the information regarding what actions can be taken against these activities through the tools, this question was asked. Therefore, to add these features in the tools when integrated in future, these results can be referred. Participants responses are discussed below.

* Participants mostly generate tickets for the application security team. They use to analyse the tickets and give resolutions accordingly. Deployment if the counter patches as per the problems occurred are the basic flow of work they follow.
* In case of any serious issues, developers report the scenario to cyber-crime department for further investigations. On the other hand, in normal error resolution, support team sometimes develop the patches accordingly, test it in the scenario and implement it on the systems. Moreover, these tools auto-deploy the patch where needed.
* Tools such as Amazon Cloudfront auto-generates the security patches for the small scale errors if any. But in case of major issues or in case of network issues, analysts manually trace the path by calling an end to end verifications within the applications. This provides the exact location of the port where they are getting the error. Then analysers use to kill the processes which might harm the systems and then close the ports.
* In some cases, developers insist staff to change their login details of each tool they use daily. Also, continuous safety policies include the testing of systems such as hardware requirements testing and Computer System Validation process. Analysts conduct the mandatory pieces of training monthly for all the staff working on the floor.
* First of all, stop the service or application to avoid further risk. Unless and until the issue is resolved, developers don’t start the application again. By deep analysis of the activities, developers generate the patch to resolve the issue in the base code.
* In the case of human errors, manually analyse the codes to detect the errors. Participants look into such situations and rebuild the code according to their needs.
* Patching and security updates according to the scenario are the line of action for such malicious activities.
* The application has to be cared with 360 degrees, that it should stand against all vulnerabilities. If patches are seen, the application needs to be stopped for further problems and patches should be removed by using security tools and required synopsis.

**Question 11: Have you observed any malicious activities due to API vulnerabilities?**

In this research, Application Programming Interface is observed that if it can be used as an entry point to enter into the system with unauthorised access. Hence, the question was asked to the participants regarding such activities observed due to the API vulnerabilities. And the results are mentioned below in the graph.

Figure 15 Pie chart of the ratio of participants observation of malicious activities due to API

The graph shows that, amongst all the participants, 80% of them are strongly agreed with the case that the APIs are responsible for these vulnerable activities. The results show that no one disagrees to the question that whether APIs are responsible or not. Therefore, it shows the importance of the security of interfaces. Literature section 2.2.2 and 2.2.3 also shows how APIs can be hacked and used as a gateway for the unauthorised access to the database.

The responses of the respondents were as follows:

* During network testing, internal calls in the applications won’t connect if the interface is not working properly. Hence, at that time analysers ping the end location to find the routers or the API which is causing the error.
* Every API is not completely safe and secured, sometimes the malicious activities in the source code of some open-source AIPs have been observed. Reason behind that is the open features; for example, if someone accidentally missed disabling the service after use; this can open the doors of a system for attackers.
* Wireshark tool helps to trace the exact location of the error too.
* Due to lack of time to time patching activity causes the formation of loopholes in the system which is, in turn, causes multiple kinds of attacks on the system.
* Since the API vulnerabilities alter the data usage and Wireshark provides the greater checks in understanding the same. The observed malicious attack is due usage of GET request and with the HTTP request.

**Question 12: During the observation of attacks, what percentage API bugs are responsible for attacks?**

This Question has been asked to check the rough percentage of the reviews of participants and to graphically analyse whether everyone is aware of vulnerabilities due to API bugs. Line graph below explains that whether everyone is on the same page or not.

Figure 16 Attacks percentage due to API vulnerabilities as per the participant's observations

According to the results of interviews, it has been clearly seen that the feedback of all the participants was different and from the zigzag format of the graph says that, not everyone is aware of the importance of the vulnerability incidents due to insecure API. With reference to the OWASP API SECURITY TOP 10 mentioned in the literature section 2.2.3, API can be vulnerable if these top 10 scenarios were not properly being analysed.

Few participants responded that:

“Not every API is fully secured and yes they might provide a gateway for attackers to enter into the system if in case the API is vulnerable.”

“It is really very hard to say the exact percentage of API bugs in the system but I must say that yes it is very important to secure the Applications Interfaces and overall applications by using tools in the work environment. Database is one of the sensitive parts of the pharmaceutical industries. Hence, it should be protected against attacks.”

## *6.1 Analysis of Vulnerability Scanning Tools:*

According to the research of the OWASP vulnerability tool scanners and the results fetched by the qualitative analysis, DAST tools are more frequently referred tools in the market. (OWASP, 2019)

Observed list of the available tools in the market, has their own strengths and weaknesses. Here, are the most rated tools by the candidates interviewed and the strengths and weaknesses of the most commonly used tools are given below.

**Wireshark:**

Table 1 Wireshark Advantages and Disadvantages

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| No need for high-end specifications, as the tool runs smoothly on legacy systems. | Lack of learning resources in the tool for new users. Eg: User guide or manual. |
| Filter functions improve efficiency and reduce time to detect the target. | Lack of optimization as the large packet size reduces the speed or the performance of the overall system. |
| The integrated tools inside it can be used for deep analysis of the different network issues. | The crowded presentation of data makes it confusing for users to understand the data. |
| Can be installed on any operating system such as Linux, Mac, Windows. |  |
| This can capture packets from multiple Network Interface Card’s (NIC’s) and provide dumps very easily. |  |

**AppTrana:**

Table 2 Apptrana Advantages and Disadvantages

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| Identifies the risk factor of the code and immediately deploy the patch. | There are no disadvantages received from the interviewees. |
| It has been built on AWS. |  |
| Improves application performance immediately. |  |
| Easy to integrate with web applications for end to end protection. |  |

**Acunetix Web Vulnerability Scanner:**

Table 3 Acunetix WVS Advantages and Disadvantages

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| Categorized as a vulnerability scanner, penetration testing and DAST (Dynamic Application Security Testing) | Lack of static review process. |
| Available as Accunetix online and Accunetix On-Premise. | Audit webservice is not active or allowed in the latest version. |
| Easy to use and multiuser web interface. | Scans become slow sometimes while running on the internet. |
| It supports documents of any format and keeps them safe. |  |

**Amazon Cloud Front:**

Table 4 Amazon Cloud Front Advantages and Disadvantages

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| Categorized as Enterprise Content Delivery Network (eCDN) and Content Delivery Network (CDN). | Complicated cache memory. |
| Integrated with AWS, Web Application Firewall (WAF) and Advanced AWS shield to defend DDoS attacks and other refined threats. | Technical support is available only for an additional fee. |
| OAI (Origin Access Identity), most widely used Security feature in Amazon Cloud front. | It is hard to calculate monthly costs as it is not that cost-efficient. |
| Simple, faster delivery, hugely configurable and flexible user interface. |  |

**Imperva Cloud Application Security:**

Table 5 Imperva Cloud Application Security Advantages and Disadvantages

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| Categorised as Cloud DDoS mitigation, Content Delivery Network and Web Application Firewall. | This tool is very expensive therefore not many people use this. |
| It can protect systems from all types of attacks. | Imperva does not offer SSL service for free. |
| Services will not affect the performance of systems while running on web application. | Lack of Graphical User Interface. |
| Easy to deploy and use. | Weak in filtering and analysis of logs. |

## *Summary of Interviews:*

From the analysis of the data, it can be understood that not every application security testing tool is fully perfect to rely on but there are solutions for this problem and for that the use of hybrid models can be an answer. Also, instead of using multiple tools, the use of hybrid models will be more beneficial to reduce the risk of data loss.

# CONCLUSION AND RECOMMENDATIONS:

The current research was carried out to determine the importance of application security testing tools being used in the pharmaceutical as well as healthcare industries with regards to the database security. Data security is not only observed in one particular country but it is the problem faces by the organizations worldwide. Hence, the aim of this research was to propose results and recommended solutions which can be used worldwide and more focused on the analysis of application security tools which can be used for the application testing in the runtime environment to avoid cyber-attacks.

The interpretivism research philosophy and the inductive research approach were used to perform the research. Qualitative research method was employed in this study. The primary data collection method was used to collect research data using the interview. Judgemental or purposive sampling method has been used. The sampling method was used to select the research sample of 9 employees who were interviewed. All the participants were experts in the testing field and are having a great experience in such field. The following are the conclusions that can be observed from the research.

**Can integration of top-rated Application security testing tools make a difference when it comes to data security?**

This question helped to understand the overview or the idea behind the use of application security tools and the integration of the application security tools for the improvement of security solutions of the applications. The motive behind this question was to find out if the integration of these tools can reduce the risk of data breaches in the pharmaceutical and healthcare industries. And this aim was achieved by the qualitative analysis process. During the research, questions were asked to the experts in the testing team and the results agree with the fact that integration of such top-rated application security testing tools will make a difference but there are few things which need to be taken into consideration while integrating the tools such as the compatibility of the systems, cost efficiency, legal aspects and FDA guidelines should be considered, and to use the SAST, DAST, IAST and RASP as a base for integration of tools (Refer to section 6). On the other hand, it is found that the concept of hybrid applications is being used such as SIEM tool by many organizations and the developers are innovating new ideas for their organizations. The common problem which pharmaceutical industries are facing nowadays is the lack of resources in small scale organizations, selection of right tool for systems, security policies etc.

**What are the current issues companies are facing due to Application Programming Interface as well as web application Vulnerabilities which leads to the data breach?**

The reason behind this question is to find out the current trending issues companies are facing due to Application Interface vulnerabilities. As the applications used in the environment of the healthcare and pharmaceutical organizations can be used as a gateway to get into the database. The results of interviews explained that there are a plethora of reasons due to which the API, as well as web applications, are being used for the cyber-attacks. Companies are facing database security issues and the respondents also mentioned the reasons behind that. The problem is due to lack of application security testing tools, lack of resources and management and human errors are causing these security issues in healthcare and pharmaceutical industries.

**How these integrated tools will help to minimise the risk of data loss and to protect the pharmaceutical as well as healthcare industries from the attacks such as Ransomware? What are their advantages and disadvantages?**

During the interviews, majority of participants said that “Not every security testing tool is perfect”, hence instead of using multiple tools, integration of two tools will be the future idea to improve the quality of security testing tools. Here, in this case, this question aims to find out the benefits of different tools and their weaknesses by which the comparison of the tools taken place to finalise the exact tools to integrate for the future work. This comparison of advantages and disadvantages will also be helpful for the organizations who are facing difficulties while selecting the perfect application security testing tool for their organization to overcome the security challenges. The results of this analysis have been mentioned in depth into section 6.2, which says that every tool has its own advantages and disadvantages. Companies should consider or use the correct tool according to their needs and must follow the policies to protect their database from attack scenarios. The most important advantage of these tools is that it can scan the systems in runtime and auto-generate the counter queries in case of any malicious activities observed.

## *7.1 Further Recommendations:*

On the basis of the results of the study which is generated by this research, there are some recommendations to improve the performance as well as to reduce the risk of data breach mentioned below.

**Awareness of API vulnerabilities and the OWAS API security top 10** –

It was observed that not every organization is facing API issues, but this should not be ignored when it comes to database security. Organizations should consider these reports every time while scanning the systems. There are precautions mentioned in the OWASP report accordingly organizations should modify their systems in the work environment.

**Follow FDA Guidelines –**

US FDA generates the report in which all the responsibilities of a good systems have mentioned. Organizations should use this guide and service such as Computer Validation System. According to which is the organizations can check and verify the current systems which are in use are good for performance improvement.

**Reduce Human Errors by improving policies –**

It has been observed that human errors can lead to the data breach and can cause a huge impact on the business. Therefore, it has been concluded that the organizations must improve the policies as well as follow them in the work environment to minimise the risk of a data breach. Organizations should implement the security awareness pieces of training as well as exams for the use of these tools which can improve the knowledge of the staff and it will be helpful for them to revise the knowledge of the tools.

**Management of resources –**

Even if the organizations have limited resources, then it should be analysed and managed properly according to the requirements so as to reduce the over costing. Workload balancing also can be taken into consideration to reduce the risk of data loss.

**Use of hybrid models or the integration of tools –**

Use of hybrid models which are currently available in the market or the development of the tools based on the DAST, IAST, SAST and RASP can be more beneficial for the organizations. Integration of DAST, IAST and RASP will increase the system compatibility of the tools which are being used in the work environment. On the basis, if the results of the interviews, it has been observed that the tools such as Apptrana and Wireshark have more benefits and organizations are preferring these tools because of the advantages it gives. Therefore, the idea of integration of these two tools by taking cost and system compatibility into consideration it seems to be beneficial for future work. There are multiple benefits of these tools but if in case of combination or the integration, it will be an added advantage for the small scale organizations also. Organizations then can use a single tool which is having the dynamic advantages when it comes to the security point of view. On the other hand, while developing the tool, cost efficiency is the factor which should be taken into consideration as the organizations are facing more issues with the cost of such tools.

# Works Cited

Adu, P. (2016, Januaary 31). *NVIVO, Perfecting the art of qualitative coding*. Retrieved December 13, 2019, from qsrinternational : http://www.qsrinternational.com/nvivo/nvivo-community/the-nvivo-blog/perfecting-the-art-of-qualitative-coding

Collinsm H. (2010) “Creative Research: The Theory and Practice of Research for the Creative Industries” AVP Publications

Davide Balzarotti, M. C. (2008). *Saner: ComposingStaticandDynamicAnalysisto ValidateSanitizationinWebApplications.* USA: University of California, Santa Barbara .

Dr Apoorva B.M, D. K. (n.d.). *Softwares used in pharmacovigilance and clinical trials.* Davangere: S.S Institute of Medical Sciences and Research Centre .

Dr. W. Liu, D. E. (2013). e-Healthcare Cloud Computing Application Solutions: Cloud-enabling Characteristices, Challenges and Adaptations. *2013 International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium .* Chico: School of Science and Technology Georgia Gwinnett College, .

Elliott, V. (2018). *Thinking about the Coding Process in Qualitative Data Analysis.* UK: The Qualitative Report, University of Oxford.

Huda Elmogazy, O. B. (2013). Towards Healthcare Data Security in Cloud Computing. *The 8th International Conference for Internet Technology and Secured Transactions .* Saudi Arabia: King AbdelAziz University J eddah.

Lu, Z. (2009). *Information technology in pharmacovigilance: Benefits, challenges, and future directions from industry perspectives.* CA, USA: Dovepress Open access to scientific and medical research.

M, A. B. (2018, june). *Review of the softwares used in pharmacovigilance and clinical trials.* Retrieved from Ommics International: https://www.omicsonline.org/abstract/review-of-the-softwares-used-in-pharmacovigilance-and-clinical-trials

Macy, J. (2018, October 01). *The importance of APIs in public cloud security: How secure do you think yours are?* Retrieved november 23, 2019, from cloud computing news: https://www.cloudcomputing-news.net/news/2018/oct/01/importance-apis-public-cloud-security-how-secure-do-you-think-yours-are/

Mohamed Elhoseny, A. A. (2018). A hybrid model of Internet of Things and cloud computing to manage big data in health services applications. *FutureGenerationComputerSystems*.

Omprakash G. Bhusnure, K. S. (2016). COMPUTER VALIDATION AND ETHICAL SECURITY MEASURES FOR PHARMACEUTICAL DATA PROCESSING . *World Journal of Pharmaceutical Research* .

OWASP. (2019, November 12). *Category:Vulnerability Scanning Tools*. Retrieved December 8, 2019, from OWASP: https://www.owasp.org/index.php/Category:Vulnerability\_Scanning\_Tools

Paper, W. (2014). *Protecting Your APIs Against Attack and Hijack .* CA Technologies.

Pitman, D. (2019, June 27). *Cybersecurity in healthcare: assessing the cyber-fitness of the health industry.* Retrieved December 1, 2019, from GDPR Priv Sec Report: https://gdpr.report/news/2019/06/27/cybersecurity-in-healthcare/

Project, O. A. (2019). *OWASP API Security Project.* Retrieved decembe 2, 2019, from OWASP: https://www.owasp.org/index.php/OWASP\_API\_Security\_Project

Reading, D. (2018, October 9). *GAO Says Equifax Missed Flaws, Intrusion in Massive Breach.* Retrieved November 12, 2019, from Dark Reading: https://www.darkreading.com/attacks-breaches/gao-says-equifax-missed-flaws-intrusion-in-massive-breach/d/d-id/1332776

Ritesh Bhangale, S. V. (2017, October 8). *A day in the life of a pharmacovigilance case processor.* Retrieved October 1, 2019, from NCBI: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5654220/

Roma Chauhan, A. K. (2013). Cloud Computing for Improved Healthcare: Techniques, Potential and Challenges. *The 4th IEEE International Conference on E-Health and Bioengineering .* India: IEEE.

Sanjay P Ahuja, S. M. (2012). *A Survey of the State of Cloud Computing in Healthcare .* Jacksonville, USA: School of Computing, University of North Florida.

Santos, W. (2019, July 17). *APIs show Faster Growth Rate in 2019 than Previous Years.* Retrieved december 1, 2019, from programmableweb survey: https://www.programmableweb.com/news/apis-show-faster-growth-rate-2019-previous-years/research/2019/07/17

securitycommunity.TCS. (2017). *10 Major security threats in cloud computing.* Retrieved April 4, 2019, from security community TCS: https://www.securitycommunity.tcs.com/infosecsoapbox/articles/2017/02/14/10-major-security-threats-cloud-computing

Syarifuddin Dollah, A. A. (2017). *Benefits and Drawbacks of NVivo QSR Application.* Makassar: ResearchGate.

Team, S. E. (2015, March 31). *Synopsys Software Integrity Blog.* Retrieved November 20, 2019, from Synopsys: https://www.synopsys.com/blogs/software-security/hybrid-application-security/

Tonuchi Joseph, E. (2019, June 29). *Analysis of Saunders Research Onion*. Retrieved december 8, 2019, from thesis mind: https://thesismind.com/analysis-of-saunders-research-onion/

Tsern-Huei Lee, M. (2013). Design and Implementation of Cloud API Access Control Based on OAuth. National Chiao Tung University, Hsinchu, Taiwan.

WHO. (2019). *World Health Organization*. Retrieved December 5, 2019, from World Health Organization: https://www.who.int/medicines/areas/quality\_safety/safety\_efficacy/pharmvigi/en/

Worrall, J. (2019, April 12). *Application & Infrastructure Risk Management: You've Been Doing It Backward.* Retrieved November 16, 2019, from Dark Reading: https://www.darkreading.com/risk/application-and-infrastructure-risk-management-youve-been-doing-it-backward/a/d-id/1336455

Xiang Fu, C.-C. L. (n.d.). *A String Constraint Solver for Detecting Web Application Vulnerability.* Hofstra University, Illinois State University.

Xiang Fu, K. Q. (n.d.). *SAFELI – SQL Injection Scanner Using Symbolic Execution.* GA : Georgia Southwestern State University, Southern Polytechnic State University .

Yao-Wen Huang, F. Y.-H.-Y. (2004). *Securing Web Application Code by Static Analysis and Runtime Protection .* NY, USA: National Taiwan University, Academia Sinica, RWTH Aachen.

Yao-Wen Huang, F. Y.-H.-Y. (n.d.). *Securing Web Application Code by Static Analysis and Runtime Protection .* Taiwan, Germany: National Taiwan University,Institute of Information Science, Academia Sinica ,Department of Computer Science, RWTH Aachen Aachen.

# APPENDICES:

## Appendix 1 INFORMED CONSENT FORM

**PROJECT TITLE:**

**Data Security in Pharmaceutical and Healthcare: Analysis of Necessary Web Application Security Testing Tools**

PROJECT SUMMARY:

This research is to identify the importance of application security testing tools which are being used and the problems faced by the pharmaceutical and healthcare industries in terms of data security. The aim of this research is to innovate an idea of integration of trending application security testing tools which can be used in every pharmaceutical industry, mainly to secure the pharmacovigilance department who deals with sensitive data against vulnerable activities. Healthcare organizations face challenges accessing and sharing data due to the cyber-attacks or the vulnerable activities in the source code such as cross-site scripting and SQL injections.

Data sets use different formats, making interoperability between apps challenging. This research aims to propose and implement integration concepts of testing tools so as to reduce the data breaches and data loss via APIs and other hacking techniques.

Time delay of medical requests such as waiting time, turnaround time of medical requests and the waste of resources utilization can be avoided if an effective mechanism is used to manage the data in a cloud environment. This can be done by the integration of application security testing tools which can improve the performance and security for software used in PV. As the PV deals with sensitive data of the patients, which has to be secured and the time to respond the queries has to be less as possible. Therefore, in conclusion, this research is expecting to propose the importance of security testing tools and innovative idea of integration of observed and trending testing tools for every organization especially the pharmaceutical industry so as to prevent any suspicious activity within the daily work environment.

By signing below, you are agreeing that: (1) you have read and understood the Participant Information Sheet, (2) questions about your participation in this study have been answered satisfactorily, (3) you are aware of the potential risks (if any), and (4) you are taking part in this research study voluntarily (without coercion).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Participant’s signature Participant’s Name

Pavan Pardeshi Pavan Pardeshi

Student Name (Printed) Student Name signature

## Appendix 2 INFORMATION SHEET FOR PARTICIPANTS

**PROJECT TITLE**

*Data Security in Pharmaceutical and Healthcare: Analysis of Necessary Web Application Security Testing Tools.*

You are being asked to take part in a research study on Data Security in Pharmaceutical and Healthcare: Analysis of Necessary Web Application Security Testing Tools. The aim of this research is to innovate an idea of integration of trending application security testing tools which can be used in every pharmaceutical industry, mainly to secure the pharmacovigilance department who deals with sensitive data against vulnerable activities. Another aim of this research is to propose a guide to refer while selecting application security testing tool for organization and to innovate an idea of integration of tools. My name is Pavan Pardeshi and I am pursuing MBA Cloud Computing at Dublin Business School. The research topic on which I am currently working is being supervised by our professor Tom Wall.

NOTE: The authorization of this topic will be obtained on 30th September 2019.

**WHAT WILL HAPPEN**

In this study, you will be asked to provide a few information regarding the work environment in the organization and the questions will be asked to answer. The research questionnaire is based on the current issued faced by experts in Pharmacovigilance department and IT department. After analysing the data retrieved through these questionnaires, the detailed theory of the importance of application security testing tools will be proposed which then can be used in the healthcare and pharmaceutical industries to prevent data loss and vulnerable activities by inventing the integrated tools based on the advantages and disadvantages. This research also helps to every healthcare industry to determine the loopholes in their current system and to maintain the records of the clients and patients safely. The personal information provided by you will not be disclosed in any case.

**TIME COMMITMENT**

The study typically takes two days from the consent form approval to the final interview. During this, if the consent form is accepted then according to the time provided by you, we will be conducting a session of one hour. In which all the questions will be asked face to face or on skype call and the data will then be recorded to summarise it in the research afterwards. This can also be done by telephonic call, skype call or over the email as per your convenience.

**PARTICIPANTS’ RIGHTS**

You may decide to stop being a part of the research study at any time without explanation required from you. You have the right to ask that any data you have supplied to that point be withdrawn/destroyed.

You have the right to omit or refuse to answer or respond to any question that is asked of you.

You have the right to have your questions about the procedures answered (unless answering these questions would interfere with the study’s outcome. A full de-briefing will be given after the study). If you have any questions as a result of reading this information sheet, you should ask the researcher before the study begins.

**CONFIDENTIALITY/ANONYMITY**

The data I collect does not contain any personal information about you except the answers provided by you during the interview session. This data will only be used in the dissertation and not for any other purpose such as presentations at conference or publications etc.

**FOR FURTHER INFORMATION**

I or/and Tom Wall will be glad to answer your questions about this study at any time. You may contact my supervisor at tom.wall@dbs.ie or DBS phone number: (01) 417 7500.

## Appendix 3: Interview Questions

1. What are your key responsibilities in the organization?
2. Which application security testing tools are currently being used and more reliable in pharmaceutical industries?
3. Amongst all these tools, which application security testing tools do you use in daily work routine?
4. How do these tools work? What are the patterns these tools follow?
5. How do you rate these tools when it comes to data security?
6. What are the current issues pharmaceutical industries are facing in terms of data security? What are your observations?
7. Over the advantages and disadvantages of these tools, what should be done to minimise the data loss?
8. Can we use hybrid models of application security testing tools instead of relying on multiple tools for vulnerability scanning? How?
9. How do you analyse malicious activities?
10. What actions do you take against these malicious activities to minimise the risk of a data breach?
11. Have you observed any malicious activities due to API vulnerabilities?
12. During the observation of attacks, what percentage API bugs are responsible for attacks?