Nat. Volatiles & Essent. Oils, 2021; 8(5): 2149-2160

NVEO
Natural Volatiles &
Essential Oils

Implementation and Mitigation for Cyber Attacks with proposed OCR Process Model

[1]Dr. Rajkumar Banoth, [2] G Arunakranthi,[3]Priyank Vachhani, [4]Shreya Kalaria, [5]Rajkumar Rathod

[1] Senior IEEE Member, Associate Professor, Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India. E-mail: naaniraj@gmail.com

[2] Associate Professor, Vaagdevi Engineering College, India

[3,4,5] IEEE Student Members, Student Graduates, Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India

Abstract

Technological innovation is rapidly accelerating in a Cyber world that is powered by social networks, online transactions, cloud computing, and automated processes. The technology evolution often brings it with the advancement of cybercrime. Which leads to Evolve in Security tools, techniques, and attack types, allowing attackers to penetrate more complex, even while remaining undetected. To make our systems more secure, it is crucial to know about those attacks, before and after they occur. Cyber security experts suggest that it is hard to predict an attack without knowing how vulnerable a network is. Therefore, it is important to analyze a networkto determine top vulnerabilities, which can give the best idea of how to shield the network. It is the ever-evolving nature of Cyber Attacks that represents the main challenge of cyber security specialist. In this paper, we will discuss the importance of cyber security and the different risks that are present in the current security era. We will also evaluate countermeasures that can be implemented when attacks occur with the proposed process model of File Upload Vulnerability. This research also seeks to identify vulnerabilities through attacks and to provide mitigation for those vulnerabilities.

Keywords: Cyber Attacks, Cyber Security, Mitigation, OCR Process Model, Security Analyst, Vulnerabilities.

I. Introduction

In cyberspace, cyber security refers to protecting systems connected to the internet from threats. The objective is to protect software and data, as well as to prevent cybercriminals from gaining access to devices and networks [1]. Cyber security is important because it ensures the privacy, security, and integrity of information, data, and devices. Today, people store excess amount of data on their computers and other internet-connected devices suchas Local Database and cloud, etc. It includes sensitive information, including passwords or financial information [2].

Keeping data, finances, and intellectual property secure it is essential for businesses and individuals. Cyber security is vital for maintaining communication and security in government and public services. In today's Cyber world, nearly every industry, government and even financial institution now uses the Internet for their transactions due to the increasing trust and usage of the Internet [3]. This makes the cyber system more susceptible to Cyber Attacks.

A Cyber Attack is an attempt to disrupt, disable, destroy, or maliciously control a computing infrastructure or to corrupt data, or both [4]. Cyber Attacks target the use of cyberspace by enterprises for the purposes of stealing controlled information [5]. Cyber Attacks are becoming much more sophisticated anddiverse as technology advances. Cybercrime becomes one of the main threats in the world. In addition, there are many types of Cyber Attacks are there, the following are some of the most common ones:

***Distributed Denial-of-Service Attack**:*

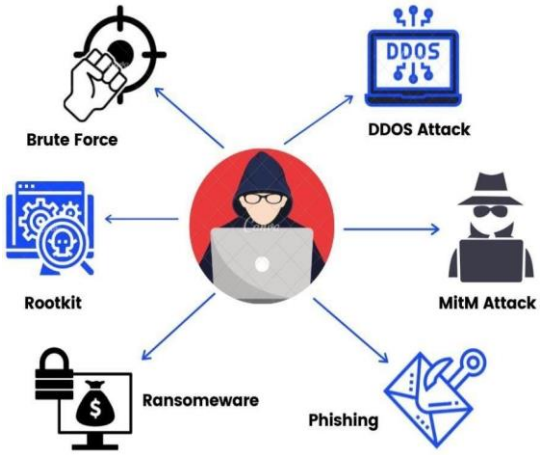


Figure 1: Various attacks

One of the most powerful internet weapons is a Distributed Denial-of-Service Attack (DDoS).Websites and online services are often the target ofdistributed denial-of-service attacks. The goal is to overwhelm them with too much traffic that can't be handled by the server or network. In order to do this, the web site or service has to be rendered inoperable [6].

***Man-in-the-Middle Attack*:**

An attacker inserts himself into a data transaction when conducting a man-in-the- middle attack (MitM). Assailants then pretend to be both legitimate participants in the transfer once they are inserted in the "middle". By doing so, an attacker can intercept any information that is passed between parties,as well as send links which is malicious to both legitimate parties that cannot be detected until they are too late [7]. Generally, there are two commonpoints of entry for MitM attacks:

An attacker can insert himself between your device and the network, an insecure public Wi-Fi connection.

The malware is injected directly into the device. Monitoring and harvesting of traffic takes place next.

Phishing:

The term "phishing" derives from the word "fishing" and uses the same tactics. An attack involving phishing is the transmission of fraudulent communications made to appear legitimate. It is done through email. An example of a fraud attack is Phishing, a scam in which hackers steal sensitive information such as credit card information and login information or install malware on the victim's computer [8].

Ransomware:

Ransomware is the most prevalent type of malware at the moment. Ransomware encrypts files or denies access to any files on an infectedcomputer system. Once the cybercriminals have gained access to the computer, they demand payment to release it [9]. There are two types ofRansomewares: i) Ransomware ii) Crypto Malware. (i) Ransomware: The only thing it does is lock your system and ask for money. (ii) Crypto Malware: As well as locking down the system, the data inside is encrypted. As soonas one paid them, they'll receive the decryption key [10].

Rootkits:

The software was installed on a compromised computer.The threat actor is provided privileged access to the system once it is installed, so it hides its intrusion and conceals its activities [11]. Rootkit is a combination of the word "root" and "kit." Under Unix and Linux, root refers to the admin account, and kit describes the software components that make up the tool [12].

Brute Force:

The objective of this attack is to allow someone to guess log-in information,encryption keys, by trial-and-error. By using all possible combinations, hackers make attempts to guess the correct combination. The attackers use brute force to try and 'force' their way into your private account(s) by using forceful methods.

Though this is an old attack method, hackers still employ it because of its effectiveness and popularity. Cracking a password depends on its length and complexity, and it can take several seconds up to many years [13].

II.Literature survey

After discussing attacks and their types above, let's now try to analyze the number of attacks organizations are facing around the globe. This figure shows the attack data that the organization has faced in the last five years. The number of unfortunate attacks has been rising over time. 2018 saw the lowest attack rate, but the power of attacks continues to increase dramatically [14]. In this article, we examine a few attack cases to show their severity, and then we propose an OCR Model to mitigate these attacks.

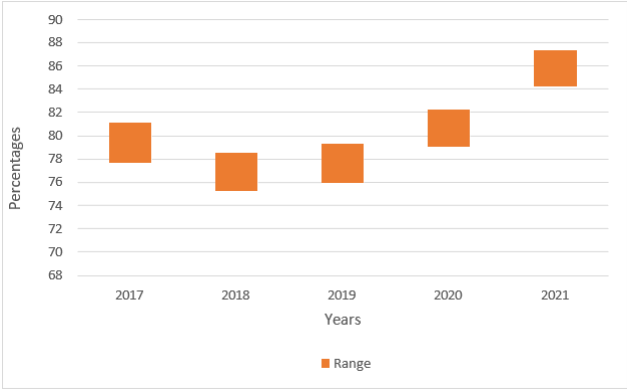


Figure 2: Attacks on organizations around the globe

Cyber attackers sometimes execute attacks successfully. There are several measures to prevent them, for instance AAA (Authorization, Authentication, Accounting). The safety of an organization can be ensured by having a secure infrastructure. The success of an attack on the MS-SQL Database occurs when the organization lacks the necessary security devices such as Firewalls, IDS, IPS etc. to prevent the attack from taking place. A robust security policy in the cyber age is important to protect the infrastructure and boost the performance of databases.

III. Related work

Organizations should maintain a strong incident response plan while goingthrough the breach of the MS-SQL database. As part of the incident response process, a team identifies the people involved in each of the various activities during the attack. Thus, it will be possible to prevent successful attacks by taking the necessary measures. In Addition, the system restricts the number of information employees can access. Organizations can keep unauthorized individuals from accessing the mainnetwork at all times.
SMB Server might contain a backup file for MS-SQL Database with guest privileges which might be vulnerable when integrated with MS-SQL Database because the local files are distributed through SMB server to the SMB clients. By displaying the vulnerability severity of MSSQL Databases and providing mitigation through the setup of Strong privacy policies and List privileges, we intend to provide an overview and mitigation of the various vulnerabilities.

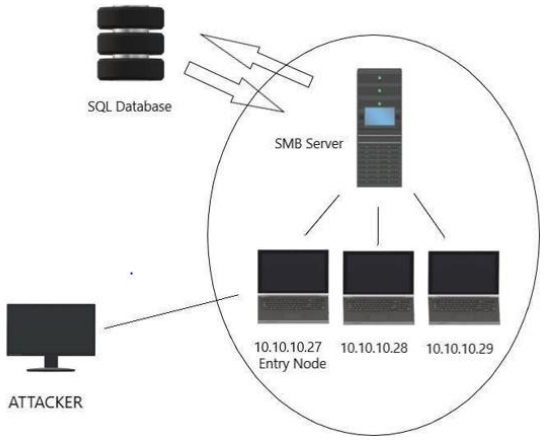


Figure 3: Architectural Diagram

A. Vulnerability Identification and Implementation of SMB Server

A security vulnerability in MSSQL Database is exploited to access thedatabase through SMB clients. Our strategy is to detect SMB servers' vulnerability to MS SQL by using enterprise networks. Cyber World consists of several end-devices, network devices, and securitydevices, all of which represent the end node for the network. The cybersecurity professionals discuss the weakness of SMB servers when viewed from the perspective of SMB clients.

A security analyst identifies vulnerabilities on the SMB Client with IP address10.10.10.27, which is the endpoint into the network. A security professional scans the SMB client devices and identifies ports and servicesthat are open on their devices.

In order to implement the initial scan, execute the command: **-sC -sV 10.10.10.27**. The scan will gather information concerning available open portsand scheduled services. These ports and services are found in the TCP protocol.

PORT	STATE	SERVICE	VERSION
-135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows Server 2019 Standard 17763
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2017 14.00.1000.00

During the scanning process, SMB Server was detected, and the entrynode revealed that it was an SMB Client with guest privileges that was connected directly to the SMB Server.

smb detected

OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)

Computer name: Archetype

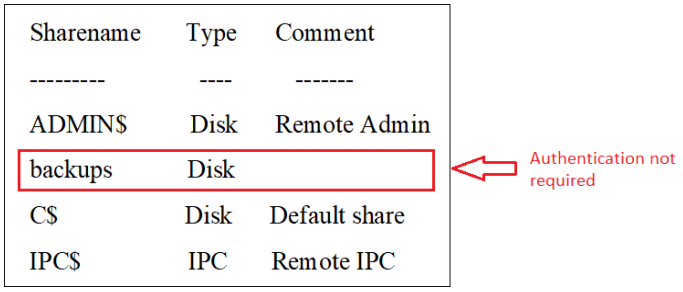
smb security :

account_used : guest ⇦ The guest user led to privilege escalation

authentication_level : user

The following table identifies which files are shared between the SMB server and the SMB Client. Disks available in the SMB Server can be seen with the command **smbclient -L $IP**. Trying to open ADMIN$ requires privilege access with appropriate credentials to gain access to the Admin Disk. There seems to be a disk with the name Backups is available. By the use of command: **smbclient //$IP/backups**, let's attempt to access it

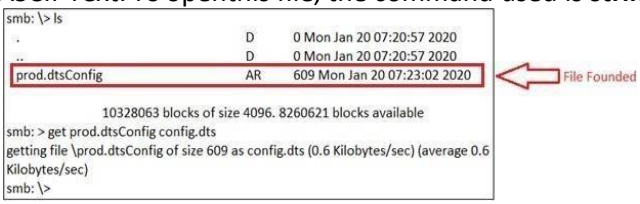
and seewhat's inside.



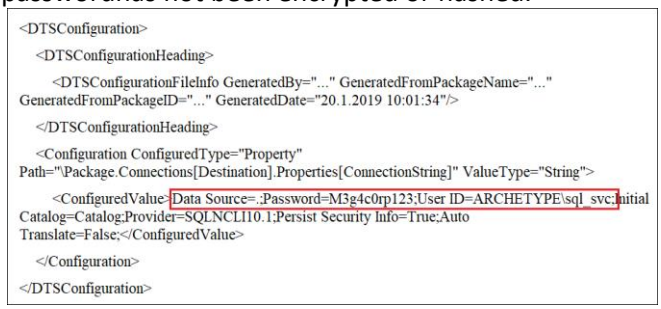
At "**backups disk**", authentication is collapsed, so a listing of backup disk files can be obtained by using the **ls** command. A file named *prod.dtsConfig* is found.

This file can be downloaded on the local system using the **get prod.dtsConfigCOnfig.dts** command where, *COnfig.dts* is the downloaded file name.

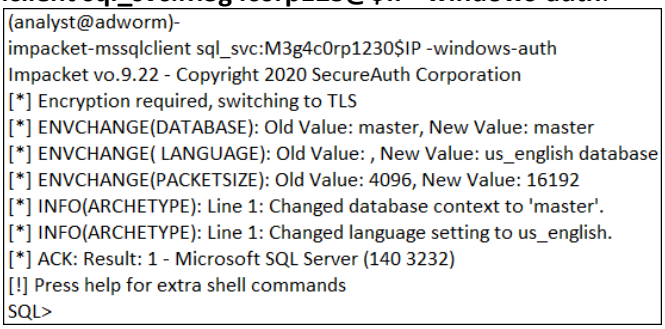
Firstly, verify the format of file with the command: **file COnfig.dts**. Having examined the information, it is evident that the file type is ASCII-Text. To openthis file, the command used is **strings COnfig.dts** .



Credentials such as User ID, Password, and Provider, that is a SQL database, are displayed upon opening of the file. Furthermore, the passwordhas not been encrypted or hashed.



The extracted credentials are used to access the MS-SQL database that was found by the scan with the command **impacket-mssqlclient sql_svc:M3g4c0rp123@$IP -windows-auth**.



The MS-SQL database contains a large number of DLL files that are shared through SMB Server over the network. To see those files **xp_cmdshell dir** command is used.

B. File Injection Attack with SMB Client on Private Network

In the current Cyber World, File Upload Vulnerabilities rank third. Uploaded files pose a significant risk to applications. File upload attacks start with the execution of code on the targeted system's database. A file upload provides an assist to the attacker in completing the first step.

If file uploads are left unrestricted, the consequences can vary, including the destruction of the system, a

completely overloaded file system, forwarding attacks to back-end systems, client-side attacks, or simple defacing. Dependingon what the application does with the uploaded file, and more specifically on where the file is stored, this can vary. Few Risk Factors are mentioned below*:*

a. By uploading and executing an executable web-shell, an attacker cancompromise a web server and run commands, browse system files, attack other servers, and exploit local vulnerabilities, etc.
b. The website becomes vulnerable to client-side attacks, such as XSS or Cross-site Content Hijacking, when malicious files are uploaded.
c. There are a variety of means by which malicious files can be uploadedto a server for later execution on an individual's computer, such as an Excel file, a windows virus, or a reverse shell.
d. The is possible that an attacker could insert a phishing page into the website or deface the website.
e. File storage servers may be utilized for hosting harmful content such asmalware, illegal software, or adult content. Also, the files may contain malware's commands and control, that can be exploited by criminal organizations.

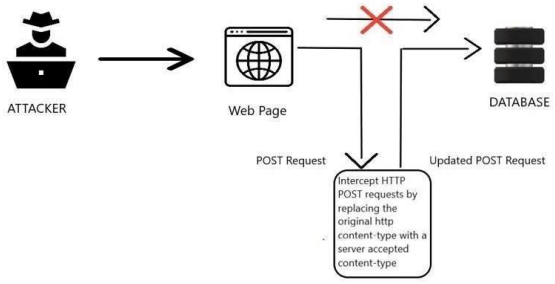
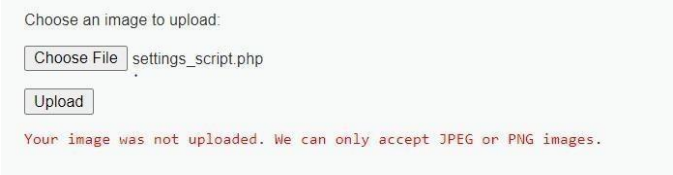
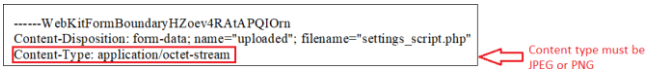


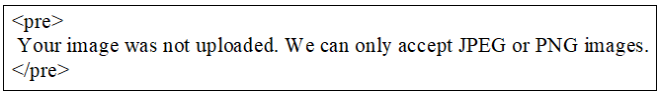
Figure 4: File Injection Diagram

In addition to the exploit of MS-SQL vulnerability, which is privilege escalation, there may also be an exploit of the file injection vulnerability. Anotable issue when it comes to online applications and SMB network is the file upload vulnerability. Cybercriminals take advantage by uploading a file with suspicious code that is executable on the server if a SMB application a web application has this type of vulnerability. In this scenario, an attacker tried to upload a php file rather than an image file, causing the database to beexploited by exploiting the input field vulnerability. As a countermeasure, we are building a system that can spot malicious content and content types through artificial intelligence.



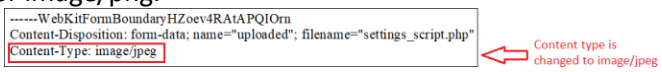
In ideal way to accept the input file is by SMB applications and web applications is based in the requirement that means SMB applications and web applications give least privileges to the user but sometime a malicious actors try to bypass these privileges by input the other files like php shell which is executable on web server if it is upload. It causes significant defacing the database. In our scenario, as a security precaution, no other content type is supported in the input field except JPEG and PNG. As a result, documents can only be uploaded to the web server when they are inrequired manner. Otherwise, they would not get uploaded.





When attacker hits HTTP POST request to the SMB server or web server;however, the server did not accept its request to upload a file with (.php) extension but before forwarding the POST request to the server for

validation attacker intercepts the POST request and change the content type to server acceptable content type, here its image/jpeg or image/png.



In terms of writing backend scripts, accepting the request and changing the content type creates the most security issues because they only validate the content type and extension not privilege type and weak security policy, but if we change either or both the script file will run on the server without the user's permission.

Our proposed OCR (Optical Character Recognition) model mitigates this type of attacks like Privilege escalation and file injection by implementingartificial intelligence and machine learning.

```
<pre>
../../hackable/uploads/settings_script.php succesfully uploaded!
</pre>
```

IV. proposed process model

The purpose of this research is to give reasonable mitigation of the attack (MSSQL Privilege escalation and File injection) we are going to propose a Process layered model for mitigation of file injection attack, which are increasing these days. Our ultimate goal is to ensure effective implementationof least privileges, privacy policies, Authentication best practices.

This research is to provide reasonable mitigation for the attacks (privilege escalation, file insertion) that are increasing these days. Our ultimate goal is to ensure effective implementation of minimum privileges, privacy policy, authentication, and best practices. We will display an OCR Process model to mitigate the file entry attack.

The OCR model has the general implementation of security that helps prevent file injection attacks because these attacks are critical to enterprise systems. There is a unit of classification that categorizes several elements of files such as content type, data, and file extension. In the database, end-users can upload files OCR model will then check for malicious code, sniper attacks, and logic bomb attacks, and whether the extension matches the actual content of the file, and whether the extension matches the type of the file.

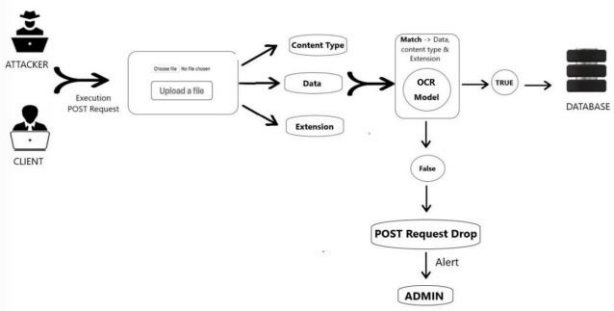


Figure 5: Architectural Diagram of the proposed process

As shown in the figure, once a user who may be legitimate or offensive interacts with the application here, we consider the SMB application to uploada file to the SMB server due to the general distribution purpose. A malicious attacker may use the file entry vulnerability to execute shell file and do some malicious things on the server through the file entry vulnerability. Security can be provided by both writing secure back-end code and performing a seriesof checks such as comparing the content type with actual content and performing secure authentication.

Here, the attacker is taking advantage of the least privileges and weak security policies applied to the client SMB that appears in the above attack, now the attacker is taking advantage of himself to exploit everything in the server SMB and if he can access the MS-SQL server as well. Through it, themalicious actor tries to put a file containing malicious code that runs independently once it has been successfully placed on the server.

But we have a Security Checker module to distinguish some attributes of the file to be uploaded like Content-type, Content, File Extension, in this moduleOCR checks if the file upload is the current file it is supposed to get by doingseveral checks like Content - type and File extension with content type compatibility with the file

extension. This is the common security system andmakes the backend understandable enough to ensure more security.

Nevertheless, in today's security world, when security is increasing every day along with that, the attacker also increases the strength and finds little space toexploit the system. So, to make sure that the system is sufficiently capable of distinguishing between a real user file and an attacker's malicious file, we willcreate a machine learning model which is learned about the relevant content and the content file with its extensions. Secures the data entry field by adding an extra layer of protection. Using an HTTP header containing the file extension, it compares actual data with the requested data type. If it finds any mismatch, it stops the file upload process and sends a notification to the parser. We are working on this issue with a best practice approach because wehave to be with the attacker's current thinking to mitigate upcoming attacks.

Once it detects that it has passed all the security checks and that it is a file thatcomes from the legitimate user, the next and important thing the SMB application does is encrypt the file with proper encryption algorithms like RSA. Because when any client registers SMB with its credentials, it generatesa key pair based on file encryption or decryption, respectively.

In conclusion, the proposed OCR model reduces the complexity of performing successful attacks and mitigates the existing vulnerability of import files input to be exploited to damage critical server or database data.

V. implementation

Since the end-user uploaded the file that should be uploaded to the databasefor use, but before storing it in the database, the administrator created a module to verify the following: 1. Data in file, 2. The file extension of file 3. Content-type(mime).

```
{ ext: 'pdf', mime: 'application/pdf' }
```

When we check the actual mime and extension, we have condition that thefile extension and the expected file mime extension match the expected mime. A match means that the item is inside.

```
if (Extracted_data.ext == Extracted_file_Data_collection && Extracted_data.mime == "application/pdf")
```

Now we need to check the data in the file. According to the extension andtype of mime, the data should be appropriate for given input field.

```
const regex = ['<?php', 'echo', 'script', 'system', 'fs', 'windows'];
```

If these keywords are present, the file will be removed from here, instead of being stored in the database because the pdf file should not contain code snippets.

There will be an alert sent to the Network Admin that something suspicioushas been detected.

```
[nodemon] clean exit - waiting for changes before restart
[nodemon] restarting due to changes...
[nodemon] starting `node index.js`
Alert : Malicous action detected
```

If the file is suitable for the expected data and there are no keywords listed inthe checker (regex), the OCR model authenticates it and stores it in the database. The content generated by the audit shows that the data was loaded successfully.

```
[nodemon] clean exit - waiting for changes before restart
[nodemon] restarting due to changes...
[nodemon] starting `node index.js`
Info : File uploaded successfully
```

A. MS-SQL Privilege Escalation Mitigations:

(a)Two-Factor Authentication:

With two-factor authentication, it becomes much more difficult for attackersto damage a person's device or account since a password alone does not suffice to gain access to a victim's digital assets. Security measures that involve two-factor authenticati on are a very common method of protecting sensitive systems and data. Increasingly, online service providers use two- factor authentication to prevent hackers from using a stolen password database to access users' credentials [16].

(b)Authentication:

To keep sensitive data safe, a hashing algorithm and encryption can both be used. Through these techniques, we can counteract this vulnerability. Moreover, Authentication with MySQL can be performed using pluggable architecture.

Many authentication methods are available, such as caching_sha2_password, and mysql_native_password.

(c)Mitigating Privilege Escalation:

Using privilege escalation vulnerabilities, an attacker can impersonate another user, open unauthorized ports, or gain unwarranted access to systemresources. Despite this, you can lower your organization's attack surface byimplementing privileged access management and identity-centric approaches [17]. The following best practices have been identified:

Vulnerability Management: Identity and fix vulnerabilities continuously, for instance through patching, fixing misconfigurations, eliminating embedded credentials, removing default credentials, etc.

Make consistent use of strong credentials management practices (discovery, vaulting, central management, check-in, check-out) both for the people and machines.

Enforce granular permissions control over access, communications, and privilege elevations within all applications with advanced application control and protection.

Implement data execution prevention that only allows codes to run in executable areas.

Be careful not to store backup files that contain unwanted information thatcould compromise security.

VI. Conclusion

As a security expert, you have to be sensitive about Cyber Attacks. A cybercriminal might use weak configurations to increase the likelihood of enhancing his activity and exploiting vulnerable devices. The emergence ofmisconfiguration has brought with it an increase in cyber-attacks. Organizations that handle confidential information, including healthcare organizations, government assets, and government affairs, are the main targets for this type of attack. In addition, these institutions have also been targeted to bring their systems down or to extort ransom before the normal operations can resume. The COVID-19 situation makes it easy for employeesto fail to comply with security measures when working at home [15].

Organizations that handle large volumes of data are targeted by the attacks. The purpose of this study was to analyses MS-SQL Database using Private Network to penetrate actual tests, in order to mitigate this vulnerability frombeing exploited by attackers. In addition to File Injection, this exploit might be used to collect data from MS-SQL Databases.

On the other side, Process model are used in many useful and applications that made our life more comfortable and smarter. Virtual infrastructure is more vulnerable to Cyber Attacks as compared to local infrastructure. Thismodel is designed to improve both efficiency and effectiveness as it combines both AI and machine-learning. To overcome cybersecurity risks to each layer, the suggested model can be coupled with security measures [18].

VII.References

[1] https://www.itgovernance.co.uk/what-is-cybersecurity#:~:text=Cyber%20security%20is%20the%20application,of%20systems%2C%20networks%20and%20technologies.
[2] https://digitalguardian.com/blog/what-cyber-security
[3] https://www.upguard.com/blog/cybersecurity-important
[4] https://searchsecurity.techtarget.com/definition/cyber-attack
[5] https://csrc.nist.gov/glossary/term/cyber_attack
[6] https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.htmlsss
[7] https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
[8] https://www.webroot.com/in/en/resources/tips-articles/what-is-phishing
[9] https://contenthub.netacad.com/cyberops/14.1.8
[10] https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/ransomware-and-crypto-

malware-2/
[11] https://contenthub.netacad.com/cyberops/14.1.8
[12]https://www.veracode.com/security/rootkit#:~:text=The%20term%20rootkit%20is%20a,components%20that%20implement%20the%20tool.
[13] https://www.kaspersky.com/resource-center/definitions/brute-force-attack
[14] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[15] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, Muhannad Quwaider "Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model" in 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)
[16] B. Rajkumar, Narsimha" Trust-based light weight authentication routing protocol for MANET "in Int. J. of Mobile Network Design and Innovation, 2015 Vol.6, No.1, pp.31 - 39.
[17] B. Rajkumar, G. Narsimha" Secure Multipath Routing and Data Transmission in MANET "in International Journal of Networking and Virtual Organizations, V16.N3. 2016.
[18] B. Rajkumar, Narsimha" Trust Based Certificate Revocation for Secure Routing in MANET "in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) Bhubaneswar, Odisha, India.

Authors Profile

Dr. B. Rajkumar, has received his B. Tech degree from National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, in the Department of Computer Science & Engineering. He has received his M. Tech and PhD from Jawaharlal Nehru Technological University (JNTUH), Hyderabad, Telangana, in the Department of Computer Science & Engineering. He has Published 18 Hi-indexed SCI and Scopus International Journals, He has Presented 6 International Conference papers and invitee speaker for 3 international conferences. Membership in Professional bodies: IEEECS senior member, The Institution of Engineers (INDIA) Member, LMISTE, MCSI, Member of Research Gate, He has awarded a CCNA and Cyber Security Operations Certified Trainer, and He is running the CISCO Networking Local Academy and trained around 4000 graduates and MNC Employees around the world. He has 15 years of teaching Experience in the Department of Computer Science & Engineering in various countries like Denmark (Europe) Ethiopia (Africa) and in INDIA, currently he is working as an Associate Professor in Marwadi University, India.

Aruna G Kranthi, an Indian, pursed her B.Tech and M.Tech from Jawaharlal Nehru Technological University, Hyderabad in Department of Computer Science and Engineering. She is an IBM Certified Trainer for Academic Associate DB2 9 Fundamentals and Application Fundamentals and, Associate Developer RAD for WebSphere Software V6.0. She has been Resource Person & Program Chair for an International Conference. Her recent research works were accepted for Elsevier and Springer Lecture Notes on IoT Decentralization and Edge Computing. She has been granted with an Australian patent. She has 15 years of teaching experience, and she is rendering her services at Vaagdevi Engineering College, Telangana.

Priyank A. Vachhani is born in Rajkot, Gujarat, India in 1998. He completed his higher education from the school named S.N. Kansagra School in Rajkot. During his high school years, he developed a keen interest in hacking and the way hackers gain access to many devices. Apart from that, he was also curious as to how security personnel analyze, monitor, and mitigate the attacks. Currently, he is pursuing his Bachelor's degree in the field of computer engineering from Marwadi University, Rajkot, Gujarat. His interests are focused on Cybersecurity, particularly as a security analyst. He is undergoing the research in Intrusion Detection / Intrusion Prevention Data Analysis. While pursuing the research, he has undertaken Cisco Cyberops Associate course to expose his skills to industrial level. Besides his research skills, he possesses a solid grounding in cybersecurity, along with technical knowledge and superior analytical

skills. He is an IEEE Student member of Gujarat section.

Rajkumar H. Rathod, was born and raised in Junagadh, Gujarat, India. He is currently studying for a B. Tech degree through Marwadi University, Rajkot, Gujarat, India, in the Department of Computer Science and Engineering. He has been a passionate and dedicated student with interests primarily in cyber security. He's also been an IEEE student member in the Gujarat section as well as having spent time interning as a MEAN stack developer at Mumbai, India. As a result, he gained an understanding of security aspects in web applications, code security, and what common mistakes developers make when developing web applications with the technical knowledge, he is having good analytical skills, self-motivated and curious to learn new things. Currently, he is doing Bug Bounty to help organizations protect themselves from potential imaging threats.

Shreya P. Kalaria, is born in Rajkot, Gujarat, India in 2000. She completed her higher education at Shree G.K. Dholakiya School in Rajkot. While she was in high school, she was curious about knowing how to protect a computer's network and its system from various types of attacks. This motivated her to learn and develop her networking skills. Her current academic endeavor involves studying computer engineering at Marwadi University in Rajkot, Gujarat. In her career she developed expertise in networking, and she started to understand how this can affect a company's security. Additionally, she is conducting research in Intrusion Detection and Intrusion Prevention Data Analysis to gain a better understanding of network infrastructure. She possesses abilities such as problem-solving skills and basic computer forensics skills that help her excel in her cybersecurity career. She is also an IEEE Student Member.