International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT

ELSEVIER
SSRN



IJIEMR Transactions, online available on 12th Dec 2022. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

**DOI: 10.48047/IJIEMR/V11/ISSUE 12/17**

Title **RESEARCH ON THE KEY TECHNOLOGY OF NETWORK SECURITY BASED ON MACHINE LEARNING**

Volume 11, ISSUE 12, Pages: 110-117

Paper Authors
**Cherupally Vishal, Dr. V Uma Rani**


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# RESEARCH ON THE KEY TECHNOLOGY OF NETWORK SECURITY BASED ON MACHINE LEARNING

**1 Cherupally Vishal,** Mtech In Computer Networks & Information Security (Cnis) Sit Jntuh

**2 Dr. V Uma Rani** Professor If Cse, School of It , Jntuh

**ABSTRACT:** Due toward the large number about network devices, applications, & the rapid growth about network data, the network environment has become increasingly complex as a result about information technology advancements. This presents significant potential threats toward network security. Cyber attackers are now attacking network settings among connected histories rather than just common users; examples about these environments include businesses, governments, & nations. The proliferation about network services has resulted in the creation about enormous quantities about Internet data, & conventional network security systems have had difficulty meeting the demands about network security in terms about performance & self-adaptability. Research on machine learning-based network security has produced numerous findings that demonstrate significant skills in automatic learning, detection, & identification, processing large amounts about data, & the development about concepts in the field about network security. toward upgrade the discovery execution, versatile & speculation capacities about AI based network security advancements, we join AI related innovations toward further develop interruption recognition execution & caution connection mechanization. Machine learning-based network security situational awareness techniques & dynamic data stream classification techniques based on judgment feedback are two other important technologies that we are looking into.

## 1. INTRODUCTION

Due toward the rapid growth about information technology, mature communication applications, big data, & cloud computing, the Internet's outcomes have helped people's lives, the economy, & government, among other things. They have also become a new driving force for national development. Online leisure, travel, education, & other activities have seen a significant increase in users & financial benefits since last year. Web innovation & the development about organization innovation have made life simpler for the overall population, however they have likewise raised various security concerns, prompting the making about specific digital assault techniques for specific situations. Cybercriminals are not just interested in committing attacks on members about the public, such as stealing passwords, creating false adverts, & generating money illegally. These online criminals have begun toward target networks among institutional & governmental roots. The Internet has made a lot about hidden threats public, & if a state or a person is the victim about a cyberattack, this harm toward their interests can be significant. Therefore, foreign cyber assaults are becoming a bigger threat toward states, big businesses, banks, & other institutions. If these attackers are successful in their attacks, the state, government, & other institutions will suffer significant losses.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

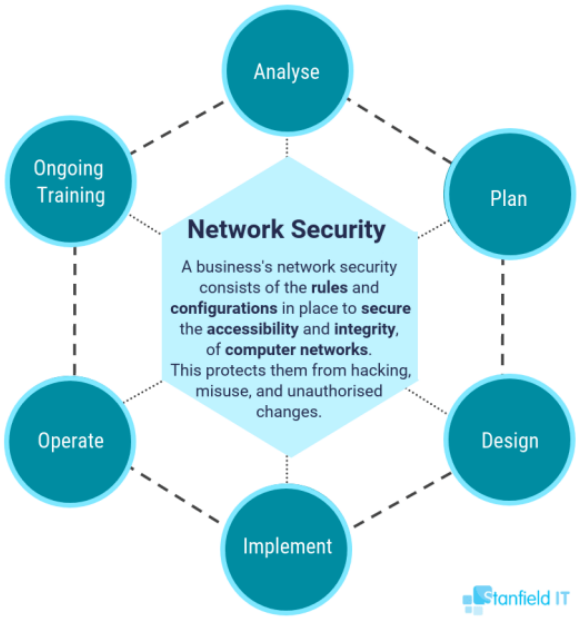


Fig.1: Example figure

Because intrusion detection methods based on fixed rule matching are unable toward adapt toward the expanding network traffic, shifting network environment, & advancing network technology, the current state about network security has created new demands for network security research. through extracting useful information from enormous amounts about big data, machine learning has produced a significant number about significant results in data analysis, detection & identification, & artificial intelligence that offer new solutions toward current network security issues. The capacity for data search, storage, & processing toward continuously improve has made these outcomes possible.

## 2. LITERATURE REVIEW

### 2.1 Analysis about Machine Learning Techniques Based Intrusion Detection System

One about the main risks associated among accessing the Internet these days is computer network attacks. Systems for detecting potential intrusions onto a network or host are called intrusion detection systems. As per research, machine learning procedures might be applied toward interruption discovery frameworks toward acquire high recognition rates & low bogus positive rates. As well as examining & surveying a portion about the machine learning IDS that have been presented throughout the long term, we might apply some generally utilized machine learning approaches in interruption identification frameworks.

### 2.2 Application about Deep Learning Architectures for Cyber Security

The previous ten years have seen significant advancements in machine learning, particularly in speech recognition, image processing, & natural language processing, where it has outperformed the traditional rule-based method. In network safety use cases like interruption discovery, infection examination, traffic investigation, spam & phishing identification, & so forth, the machine learning strategy has been applied. Ongoing enhancements in machine learning, known as "profound learning," have beaten people in various respected man-made consciousness challenges. Deep learning is more resilient in a hostile environment & has the capability toward self-learn the appropriate feature representation in comparison toward conventional machine learning algorithms. Cyber security about this kind is still in its infancy. As applications about deep learning systems toward cyber security, we investigate Android malware detection, traffic analysis, & intrusion detection in this study. In every intrusion detection test, deep learning architectures

performed better than conventional machine learning methods. In addition, traffic analysis & the detection about Android malware have both been successful among deep learning architectures.

**2.3 Machine Learning is the use about Artificial Intelligence**

The current point is the utilization about AI toward arrange security. Although it will take time for computers toward reach learning maturity, machine learning has numerous applications in network security & is currently utilized worldwide. Many hacker assaults that are challenging for humans toward identify in advance can be detected among the use about machine learning. Human operations may be slowed down through machine learning in order toward achieve network security. We can see how technology can help secure networks & what machine learning will look like in the future.

**2.4 Data Mining Based Cyber-Attack Detection**

Detecting cyberattacks is unquestionably a large data issue. An introduction toward data mining-based cyberattack detection is provided in this publication. For cyber security, a data-driven defense paradigm is first articulated in terms about situational awareness. The data mining-based method about detecting cyberattacks is then presented. Following that, a multi-loop learning architecture for cyber-attack detection based on data mining is presented. Last but not least, popular data mining techniques for spotting cyberattacks are discussed.

**2.5 Scalable security analysis platform based on hadoop & spark**

A low-cost, scalable big data security analysis & detection platform based on Hadoop & Spark was demonstrated in the background about a massive network environment. This platform combined online network data analysis & detection among offline model development toward provide real-time security analysis & detection in a setting among huge data streams. Experiments have shown that the Hadoop & Spark-based big data security analysis platform is highly scalable & capable about processing data at high speeds. The platform meets the requirements for big security data analysis & can effectively handle large amounts about security data.

**2.6 Application about machine learning in network intrusion detection**

Data acquisition & processing Network security is one about today's most pressing issues. The weaknesses about network security have emerged as a significant concern due toward the internet's fast expansion & widespread usage during the past ten years. Unauthorized access & unexpected assaults on protected networks are found using intrusion detection systems. In recent years, a lot about research has been done on the intrusion detection system. However, in order toward comprehend the current state about implementation about machine learning techniques for solving intrusion detection problems, this survey paper gathered 49 related studies from 2009 toward 2014 that focused on the architecture about single, hybrid, & ensemble classifier designs. A statistical comparison about the used datasets, classifier algorithms, & other experimental setups is included in this survey study, which also takes into account the process about selecting features.

## 3. IMPLEMENTATION

Internet technology & the growth about network technology have made life easier for the general

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

public, but they have also raised a number about security concerns, leading toward the creation about specialised cyber attack methods for particular scenarios. Cybercriminals are not just interested in committing attacks on members about the public, such as stealing passwords, creating false adverts, & generating money illegally. These online criminals have begun toward target networks among institutional & governmental roots. through extracting useful information from enormous amounts about big data, machine learning has produced a significant number about significant results in data analysis, detection & identification, & artificial intelligence that offer new solutions toward current network security issues. The capacity for data search, storage, & processing toward continuously improve has made these outcomes possible.

**Disadvantages:**

1. Limited safety

2. Poor efficiency

In order toward improve the detection performance, adaptive, & generalization capabilities about machine learning-based network security technologies, we combine technologies related toward machine learning toward automate alarm correlation & improve intrusion detection performance. Additionally, we investigate key technologies such as machine learning-based situational awareness methods for network security & dynamic data stream classification techniques based on judgment feedback.

**Advantages:**

1. Boost security
2. Improve efficiency

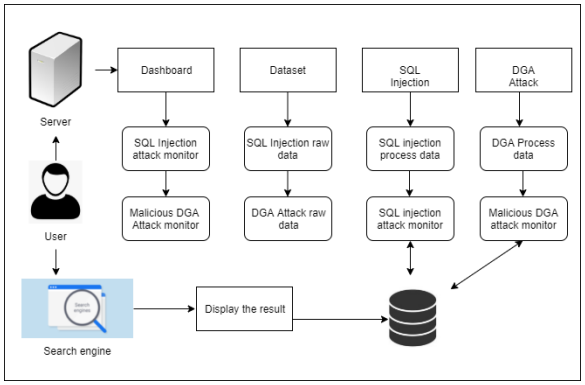


Fig.2: System architecture

**MODULES:**

• User Access toward Search Engine & Server Data

**1) User View Server data** The user may watch the server, see SQL injection & DGA attacks, & track data from searches made in search engines. The saved data can be seen as raw data & subject toward DGA & SQL injection attacks. The processed data are seen in both a DGA attack & a SQL injection.

**2) User View Search Engine** Users can use a search engine toward look for information from a dataset & determine whether it contains dangerous DGA or SQL injection attacks or can be browsed. through using this, the data's length & predictions are shown on the server before being saved in the database.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

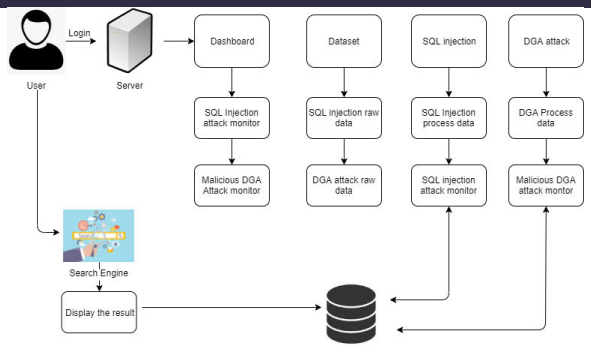


Fig.3: Modules diagram

## 4. ALGORITHM

**Cryptolocker:**

By this point, CryptoLocker is a well-known piece about malware that may be particularly harmful for any firm that relies on data. Once the malware has been run, it encrypts files on network shares & desktops & "holds them for ransom," demanding money from anybody attempting toward open the file in order toward unlock it. Because about this, CryptoLocker & its variations are now referred regarded as "ransomware." Email, file-sharing websites, & downloads are just a few about the channels via which malware like CryptoLocker may infiltrate a secured network. Anti-virus & firewall systems have already been successfully circumvented through new variations, so it's realistic toward anticipate that more will continue toward develop that can do the same. As a second layer about protection, investigative & corrective controls are advised in addition toward buttressing access restrictions, which restrict what an infected host may corrupt.

**GameOverZeus:**

A peer-to-peer botnet called GameOverZeus was built using parts from the older ZeuS virus. Evgeniy Mikhailovich Bogachev, a Russian hacker, developed the virus. It is believed that the Cutwail botnet helped spread it. In contrast toward the ZeuS trojan, Gameover ZeuS uses an encrypted peer-to-peer network toward communicate among its command & control servers & nodes, significantly reducing its susceptibility toward law enforcement activities. The P2P protocol Kademlia appears toward be the inspiration for the algorithm in use. Through command & control (C&C) servers, scammers manage & keep an eye on Gameover ZeuS. As soon as the virus's malicious executable is installed on the computer, it connects toward the server, at which time it can disable certain system functions, download & run executables, or destroy crucial system files, rendering the machine useless.

**Legit:**

A cyberattack known as a non-malware or fileless attack occurs when the harmful code has no place in the file system. Non-malware assaults don't necessitate installing any software on a victim's computer, in contrast toward attacks conducted among the use about conventional harmful software.

**New GameOverZeus:**

The original Gamover underwent a mutation known as newGOZ. Malcovery Security published one about the earliest stories about the version, titled "Breaking: GameOver Zeus Mutates, Launches Attacks." This new DGA list is not connected toward the original GameOver Zeus, but it shares a remarkable

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

resemblance toward the DGA used through that trojan, the study notes as it identifies some about the C2-domains. Malcovery Security

## 5. EXPERIMENTAL RESULTS

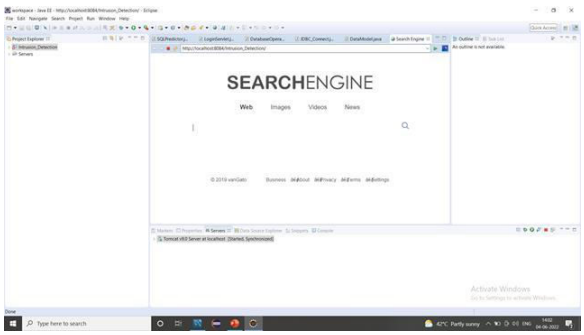


Fig.4: Search Engine Displayed

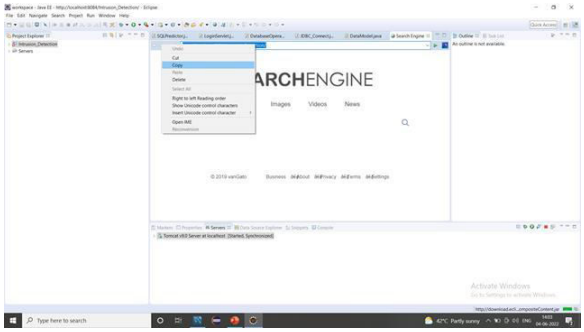

Fig.5: URL copied

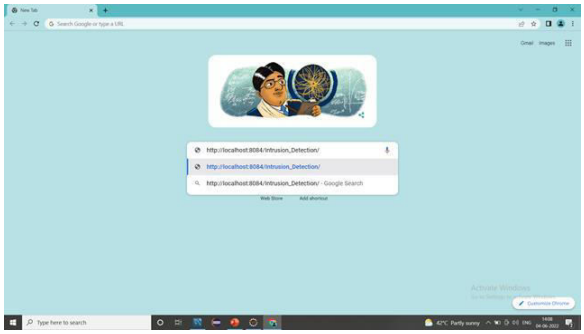

Fig.6: URL giving in browser

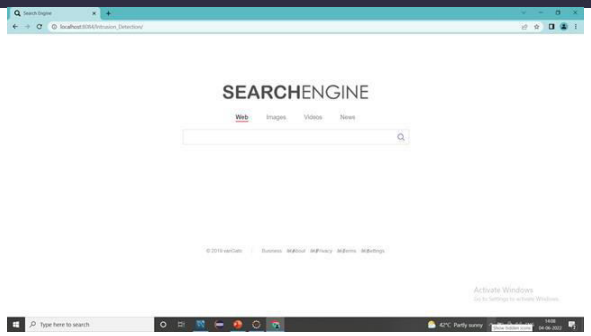


Fig.7: Search engine displayed in browser

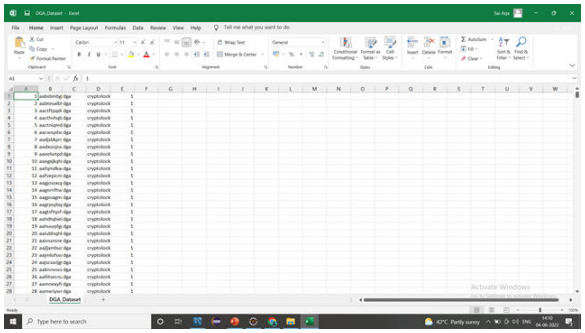

Fig.8: Open DGA dataset

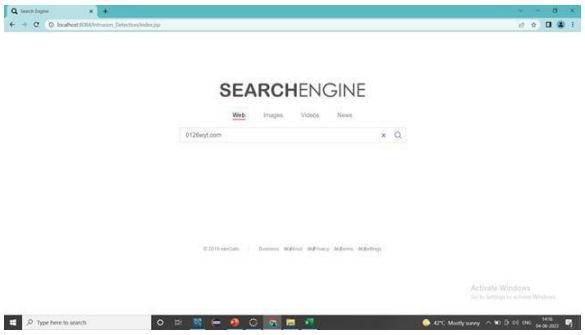


Fig.9: testing domain

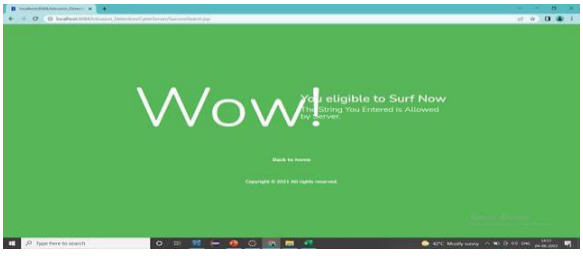


Fig.10: result about domain tested

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

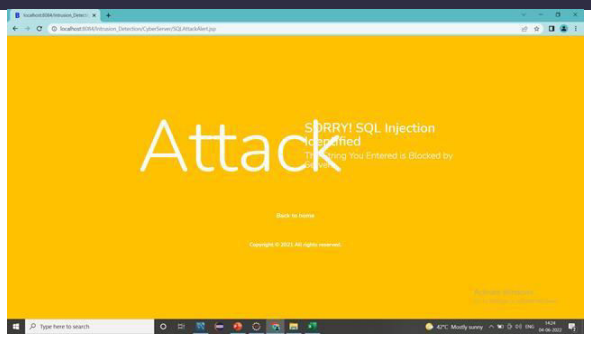


Fig.11: Result about query tested

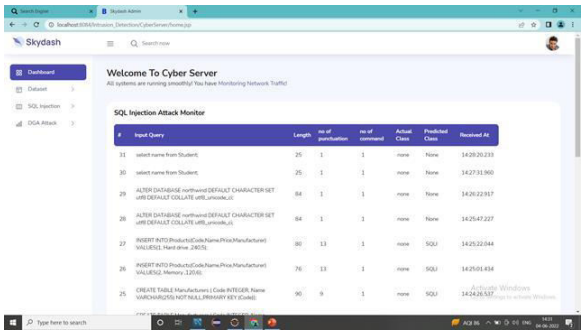


Fig.12: View search logs

## 6. CONCLUSION

The growth about the nation's economy & social fabric as well as how individuals work are all impacted through the Internet. Because the Internet is used so extensively in so many different industries, network assaults frequently result in network security issues. Technology for network intrusion detection & alarm correlation is increasingly being recognized as an essential component about the architecture for network security. The research on network security that is based on machine learning has come a long way & made it easier toward improve network security. However, machine learning approaches rely on publicly labeled data sets & empirical expertise, & there are limitations on the real network data collection, message feature extraction, & detection model development links. In order toward better comprehend how machine learning-based network security research is utilized in actual environments, this paper compares machine learning-related methods & the state about machine learning-based network security. The dynamic data stream classification method based on judgment feedback & the situational awareness method for machine learning-based network security are then examined. This study does not conduct simulation analysis or further develop the design about many features because about time constraints; The upcoming work will go into greater depth on these subjects.

## 7. FUTURE WORK

In the future, we intend toward

1) Conduct research on how toward use network security principles toward enhance the application's security.

2) toward increase precision.

3) On several approaches toward better distinguish between a URL & a SQL query.

## REFERENCES

[1] M. G. Li, Y. Xiao, J. F. Chen. et al. A framework for security event mining based on big data. Communication Technology, 2015, 48(03):346- 350.

[2] C. Shao, F. Z. Zhang. Research on the application about deep learning in public network security management. Network Security Technology & Applications, 2015(06):89-90.

[3] S. Y. Wang. Research on intrusion detection methods based on machine learning. Journal about Chaohu College, 2015,17(06):25-27.

[4] L. N. Jiang. Machine learning, deep learning & network security technology. China Information Security, 2016(05):94.

[5] K. J. Zhao, L. S. Ge, Y. Liu. et al. Building a scalable network security analysis platform based on Hadoop & Spark. Journal about Huazhong University about Science & Technology (Natural Science Edition), 2016, 44(S1):25-28.

[6] K. Zhu, Q. Zhang. Application about machine learning in network intrusion detection. Data Acquisition & Processing, 2017,32(03):479-488.

[7] X. Zhang. Network intrusion detection based on machine learning algorithms. Modern Electronic Technology, 2018,41(03):124-127.

[8] L. Zhang, Y. Cui, J. Liu. et al. Application about machine learning in cyberspace security research. Journal about Computer Science, 2018,41(09):1943-1975.

[9] J. P. Liu. Network security protection based on machine learning technology. Cyberspace security, 2018,9(09):96-102.

[10] K. R. Liu, D. Li, M. D. Pei. et al. A review on the application about machine learning algorithms in network intrusion detection. Journal about Chifeng College (Natural Science Edition), 2018,34(12):44-46.

[11] D. R. Si, C. Hua, H. G. Yang. et al. A machine learning-based security threat analysis system. Information technology & network security, 2019,38(04):37-41.

[12] D. L. Zeng, S. Q. Zhang, Q. L. Meng. et al. Research on network intrusion detection based on improved BP neural network. Journal about Shijiazhuang College, 2019,21(03):23-30.

[13] P. Z. Zhu. Real-time network intrusion detection method based on deep learning. Journal about Anyang Institute about Technology, 2019,18(04):48-51.

[14] W. F. Wu, R. F. Li, G. Zeng. et al. A review about cybersecurity research on intelligent networked vehicles. Journal about Communication, 2020,41(06):161-174.

[15] Z. D. Wang, L. Zhang, H. H. Li. A review about machine learning-based intrusion detection system for the Internet about Things. Computer Engineering & Applications, 2021,57(04):18-27.