Term Paper

On

Artificial Intelligence Techniques for network security

Submitted in partial fulfilment of the requirements
for the award of the degree
of

Bachelor of Technology

in

Computer Science and Engineering

By

Rajat Gupta
Enrollment No. A60205220088

Under the guidance of

Mrs. Amrita Parashar
Assistant Professor

Department of Computer Science and Engineering
Amity School of Engineering & Technology
Amity University Madhya Pradesh, Gwalior

November 2021

Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University Madhya Pradesh, Gwalior

DECLARATION

I, **Rajat Gupta**, student of Bachelor of Technology in Computer Science and Engineering hereby declare that the Term Paper entitled **"Artificial Intelligence Techniques for network security"** which is submitted by me to Department of Computer Science and Engineering, Amity School of Engineering & Technology, Amity University Madhya Pradesh, in partial fulfilment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

Date:-09/11/2021

Rajat Gupta
(Enroll. No. A60205220088)

Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University Madhya Pradesh, Gwalior

CERTIFICATE

This is to certify that **Rajat Gupta (Enrollment N0. A60205220088),** student of B.Tech(CSE) III semester, Department of Computer Science and Engineering, ASET, Amity University Madhya Pradesh, has written his Term Paper entitled **“Artificial Intelligence Techniques for network security”** under my guidance and supervision.

The work was satisfactory. He has shown complete dedication and devotion to the given work.

Date:

(Mrs. Amrita Parashar)
Assistant Professor
CSE ASET

(Dr. Venkatadri Marriboyina)
Head of the Department

ACKNOWLEDGEMENT

I am very much thankful to our honourable Vice Chancellor **Lt Gen. V. K. Sharma AVSM (Retd)** for allowing me to write term paper. I would also like to thanks **Prof. (Dr.) M. P. Kaushik**, Pro-Vice Chancellor, Amity University Madhya Pradesh for his support.

I extend my sincere thanks to **Maj. Gen. (Dr.) S. C. Jain, VSM** (Retd),** HOI, Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior for his guidance and support in writing my term paper. I would also like to thank **Prof. (Dr.) Venkatadari Marriboyina** Head of Department (CSE), for his kind concern throughout the term paper.

I am very much grateful to **Mrs. Amrita Parashar**, Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Madhya Pradesh my supervisor for her constant guidance and encouragement provided in this endeavor.

I am also thankful to the whole staff of ASET, AUMP for teaching and helping me always. Last but not the least I would like to thank my parents and friends for their constant support.

Rajat Gupta
(Enroll. No. A60205220088)

ABSTRACT

Networking is that a part of technology that with none doubt goes to extend day by day, however everything has its execs and cons. Therefore, for taking care of the disadvantages, varied network security protocols are established. These have helped us to associate degree extent to keep up the safety and privacy of networking. however there square measure alternative considerations too concerning the advancement of technology within the future. This analysis paper is written with the thought to dig out issues that the globe is facing and the problems which can be comes across the globe and can show some adverse effect on the expansion of networking. This paper also concentrate on the solutions that have the long run scope to counter these issues together with new techniques developed and devised by some researchers and network security-based start-ups incorporating AI, which can be the long run trend for resolution heaps of forthcoming problems within the technology and the system detection algorithm based on the concept of artificial intelligence has been proposed. Integrating Artificial intelligence into the field of network security can not only improve the overall performance of the network ,but also effectively and reliably guarantee the security. firstly according to the characteristics of computer network security , an immune detection algorithm is proposed to evaluate the security of the system . Secondly, based on the analysis of computer network security technology, a system detection algorithm based on artificial intelligence concept is further proposed. Then, data mining is carried out based on prefix, and the intrusion lines and their correlation are analysed. Finally the effectiveness of the algorithm is analysed experimentally. The results shows that the proposed algorithm has good accuracy and adaptability, and can play a good supporting role in the security detection of computer network security.

Keywords: AI , Network Security , Cyber Security**.**

LIST OF FIGURES

LIST OF ABBREVIATIONS

S. No.	Terms	Expanded Form
1	AI	Artificial intelligence
2	DDoS	Distributed denial-of-service attacks.
3	IT	Information Technology.
4	IPS	Intrusion Prevention System.
5	NAC	Access Control Network.
6	SIEM	Security Information and Event Management.
7	VPNs	Virtual Private Network.
8	ANN	Artificial Neural Network.
9	IoT	Internet Of Things.
10	MITM	Man In the Middle.
11	SSL	Secure Sockets Layer.
12	TLS	Transport Layer Securities.
13	SQL	Structured Query Language.
14	DLP	Data Loss Prevention.
15	CIA	Confidentiality, Integrity, Availability.

CONTENTS

CHAPTER 1
INTRODUCTION

In step with many protection analysts, protection incidents reached the highest number ever recorded in 2019. In the present scenario, networking is employed all over like in e-Commerce, resource sharing, communication through emails, etc. however with the recognition of networking, the quantity of threats has additionally exaggerated speedily. a number of the main threats round-faced with their solutions area unit malware that uses signature and heuristics detection engines to predict attack, ransomware prediction is feasible by exploitation AI-based models and keeping the systems absolutely updated, DDoS attacks area unit recovered by police investigation the traffic and credibleness of its supply by exploitation signature or anomaly detection ways, IOT threats area unit overcome by providing privacy and protection at network and repair level, phishing that desires correct access management system and AI-based detection models, man within the middle attacks are often overcome by exploitation virtual non-public networks. Some more modern threats area unit end-point attacks on cloud, type jacking, crypto jacking, spoofing etc., that area unit additional or less subsets of on top of major threats. Artificial intelligence endeavors to simulate human intelligence. It has immense potential in cybersecurity. If harnessed correctly, Artificial Intelligence or AI systems can be trained to generate alerts for threats, identify new types of malware and protect sensitive data for organizations.

CHAPTER 2
NETWORK SECURITY

2.1 Network security

Network security is any activity designed to protect the usability and integrity of your network and records.

A network contains two or a lot of machine systems connected by wire or wireless connections. Networks generally use peer-to-peer or client-server design with the exception of variety of networking protocols for the connected systems to speak with one another.

Network security can be a part of networking. Which includes securing the connected network infrastructure from the base to the sting of the network perimeter? Network Administrator is the one who ensures network security.

Network security involves uses IT security policies and deploys network package and hardware to:

a) Protect the network's infrastructure from external cyberattacks.
b) Protect all IT resources that can be obtained by the network from unauthorized access.
c) Ensure approved users have access to that network IT assets and resources to so as to work efficiently.
d) It consists of each hardware and software technology.
e) It objectives a variety of threats.
f) It stops them from getting into your network.
g) Powerful network security manages get entry to the network.

2.2 Threats of network security

A list of some most common threats to network and computer systems are as follows: -

a) Distributed denial-of-service attacks (DDoS)
b) Malware
c) Spyware
d) Adware
e) Computer worms
f) Botnets
g) Trojan horses

2.3 Works of network security

There are several layers to consider once addressing network security across a corporation. Attacks can be obtained at any layer within the network security's layer models , which means your network security hardware computer code and policies should be designed to such that they are capable to deal with every space.

Network security mainly consists of three completely different controls i.e., Physical, Technical and Administrative. This can be general description of the different forms of network security and the way every management works.

2.3.1 Physical Network Security

Physical security controls are designed to protect unauthorized personnel from gaining physical access to various network parts such as routers, cabling cabinets and so on. Controlled access, such as locks, biometric identification and different devices, is important in any organization.

2.3.2 Technical Network Security

Technical security controls shield information that is maintained on the network or that is in transit within or out of the network must ensures two things; it must shield information and systems from unauthorized users, and also must shield it against malicious activities from staff.

2.3.3 Administrative Network Security

Administrative security managements encompass security schemes that control user behaviour, as well as however users are genuine, their level of access and conjointly however IT workers members implement changes to the infrastructure.

2.4 Policy

An IT security policy ensures the foundations associate degreed procedures for all licensed people accessing IT assets and resources of any organisation. It's the principal document for ensuring network security. Its goal is to establish rules for ensuring the safety of structure assets.

Employees nowadays usually use many tools to conduct business profitably. Policy driven by the organization's culture supports these routines and focuses on ensuring the implementation of these tools for workers. Social control and watch process for any restrictive compliance to that a corporation is subject should be planned out within the policy yet.

2.5 Enforcement

Enforcement issues analysing all network traffic flow and aims to preserve the confidentiality, integrity, and convenience of all systems and knowledge on the network. Once enforcement starts implementing security, network security can be said to follow "CIA" triad:

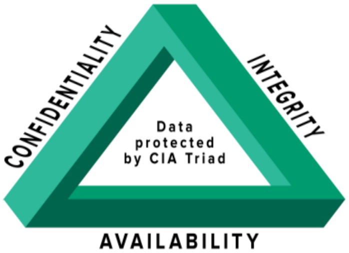


Fig 2.1 CIA Traid

2.5.1 Confidentially- Protective assets from unauthorized entities.

2.5.2 Integrity- Guaranteeing the modification of assets is handled in an exceeding mere and approved.

2.5.3 Availability- Establishing a state of the system during which approved users have continuous access to same assets.

Strong social control strives to supply United States intelligence agency to network traffic flows. This starts with a category of user flows by way of application, utility user and contents. Due to the vehicle for content material, all applications should initial be known by the firewall notwithstanding port, protocol, evasive techniques or coding. Correct application identifies full visibility which the content carries. Policy management may be simplified by discriminating applications and mapping their use to a user identity whereas inspecting the content the least bit times for the maintenance of United States intelligence agency principles.

The idea of defense exhaustive is ascertained as a best apply in network security, authorizing for the network to be saved in layers. These layers apply associate degree assortment of security management to sift out threats attempting to enter the network i.e., entrance control, identification, confirmation, malware detection, encryption, file kind filtering, URL filtering and content filtering.

These layers area unit engineered through the preparation of firewalls, intrusion hindrance systems (IPS) and antivirus elements. Among the elements for social control, the firewall (an access management mechanism) is that the base of network security.

Providing United States intelligence agency with network traffic flows is tough to accomplish with gift technology. Ancient firewalls area unit suffering from controls that trust ports and protocols to spot applications – that have currently developed evasive characteristics to grant the controls – and therefore the assumption that address equates to user identity.

Next-generation firewalls retain associate degree access management mission however re-establish the technology; they observe all traffics across every ports, will classify applications and their content, and establish staff as users. Which grants access controls nuanced enough to enforce the IT security policy because it applies to every worker of a corporation, with no compromise in security.

Auxiliary features for layering network security to implement a defense-in-depth strategy are added within the ancient model as add-on elements. IPS and antivirus, as an example, area unit effective tools so as to scan content and prevent malware attacks. However, organizations should take care of the quality and cost that further elements could increase network security and, additional significantly, not rely upon these further elements to try to the basic job of the firewall.

2.6 Auditing

The procedure of auditing network security needs checking back on social control measures to work out however well they need aligned with the protection policy. Auditing encourages non-stop improvement through requiring organizations to replicate on the execution of their policy on a uniform basis. This provides organizations the chance to regulate their policy and social control policy in areas of increasing demand.

2.7 Important Components of Network Security

Firewalls, IPS, network access management (NAC) and security information and event management (SIEM) area unit the four most essential parts of network security. Others embrace knowledge loss bar (DLP) antivirus and malware, software application, internet and Gmail security, and a lot of.

Network security is crucial in protective networks against knowledge breaches as long as just about all knowledge and applications area unit attached to a network. Having your network hacked will ruin your organization's name and place you out of business. It helps businesses mitigate the danger of falling victim of information thieving and sabotage.

2.8 AI System's Support to Network Security

Against this backdrop, organizations have started mistreatment AI to assist manage a growing vary of network security risks, technical challenges, and resource constraints by enhancing their systems' robustness, resilience, and response. AI systems work with security analysts to alter the speed at those operations is performed. During this regard, the link between AI systems and security operators ought to be understood as a cooperative integration, within which the distinctive additional value of each humans and AI systems area unit preserved and increased, rather than as a contest between the two.

Estimates counsel that the marketplace for AI in Network security can grow from $3.92 billion in 2017 to $34.81 billion by 2025, at a compound annual rate of growth (CAGR) of thirty one.38% throughout the forecast amount. According to a recent Capgemini survey, the pace of adoption of AI solutions for cybersecurity is skyrocketing. The quantity of corporations implementing these systems has risen from one fifth of the general sample in 2019, to 2 thirds of corporations aiming to deploy them in 2020. Seventy three of the sample tested AI applications in cybersecurity. The foremost common applications area unit network security, followed by knowledge security, and terminus security.

Three main categories are known in AI use in cybersecurity: detection (51%), prediction (34%), and response (18%).

The driving forces that area unit boosting the utilization of AI in Network security comprises:

2.8.1. Speed of impact: In a number of the key attacks, the common time of impact on organizations is four minutes. What is more, today’s attacks don't seem to be simply ransomware, or just targeting sure systems or sure vulnerabilities; they'll move and alter based mostly on what the targets do. These sorts of attacks impact unbelievably quickly and there are not several human interactions which will happen within the in the meantime.

2.8.2. Operational complexity: these days, the proliferation of cloud computing platforms and therefore the fact that those platforms is operationalized and deliver services terribly quickly – within the millisecond vary – implies that you cannot have plenty of humans in this loop, and you have to consider a lot of analytics-driven capability.

2.8.3. Skills gaps in cybersecurity stay Associate in nursing current challenge: in step with Frost & Sullivan, there is a world shortage of a couple of million and cybersecurity specialists. This level of scarcity pushes the business to alter processes at a quicker rate.

CHAPTER 3

HISTORY OF NETWORK SECURITY

Improving network security could be a high priority for each business and organization these days. If we glance back to the history of network security beginning around 1950, the subject began as shortly as folks started realizing that there was intrinsic worth in information. This happened in an exceedingly series of events because the info and Digital Age unrolled within the half of the twentieth century.

In the late Nineteen Sixties and into the first Seventies, digital storage became a reality. Large, room-sized mainframes were liable for storing this info and access to those storage repositories was granted by plugging directly into the mainframe itself or accessing the mainframe’s information from one amongst several terminals inside the building. Early adopters of digital storage technology didn’t have a retardant protective company sensitive info as you truly had to be within the building to induce to the data.

Less than a decade later, as a lot of and a lot of information was hold on, there was a shift in thinking: information had worth and enclosed massive volumes of in person distinctive info — master card information, checking account numbers, profit and loss statements, personal details, demographic info on massive population teams. It had been throughout this shift that info started turning into an artefact.

These were simply the first beginnings of the longer term of network security because the information revolution would continue and drive changes in security methods. Contemplate that simply five years from currently, our collective information worldwide can reach one hundred seventy-five zettabytes — onerous to imagine however massive a zettabyte really is, however as a multiple of the unit computer memory unit for digital info, simply image one hundred seventy-five followed by twenty-one zeros. This monumental volume of digital information can embrace databases, videos, photos, all kinds of apps, and far a lot of.

The fast proliferation of digital information brought with it the unexampled risk of the foremost sensitive info ending up within the hands of the incorrect folks.

The introduction of on-line access and {also the} net also accelerated this risk. Not solely did corporations have massive amounts of non-public info on staff and customers, they conjointly started sharing, marketing, selling, and repackaging this information, introducing even bigger risk and security considerations.

As information became an extremely valued artefact, each the genesis of crime began and also the fashionable approach to cybersecurity protection passed. Something with worth are often bought, sold, and most significantly, stolen. Corporations currently had to face the new reality that their sensitive info required to be unbroken safe from cybercriminals.

In fact, analysis these days shows that by 2023, over thirty-three billion information records are going to be taken by cybercriminals — a rise of a hundred and seventy fifth since 2018.

CHAPTER 4

ROLE OF AI IN NETWORK SECURITY

4.1 Detecting New Threats

AI may be used to identify network threats and, likely malicious activities. Traditional software structures clearly cannot hold pace with the sheer number of new malwares created every week, so that is an area AI can clearly help with.

By using the usage of sophisticated algorithms, AI structures are being skilled to discover malware, run sample reputation, and locate even the minutest behaviours of malware or ransomware attacks earlier than it enters the system.

AI lets in for advanced predictive intelligence with natural language processing which curate's statistics on its personal through scraping thru articles, news, and research on cyber threats.

This could deliver intelligence of recent anomalies, cyberattacks, and prevention techniques. Despite of everything, cybercriminals comply with tendencies too so what is famous with them changes constantly.

AI-primarily based community safety structures can offer the state-of-the-art expertise of worldwide as well as industry-specific risks to better formulate important prioritization decisions based now not simply on what can be used to assault your systems but based totally on what is most likely to be used to assault your structures.

4.2 Battling Bots

Bots make up a big bite of internet site visitors nowadays, and that they may be risky. From account takeovers with stolen credentials to bogus account introduction and data fraud, bots may be an actual risk.

You couldn't tackle computerized threats with guide responses by me. AI and gadget mastering help construct a radical information of internet site traffic and distinguish between excellent bots (like search engine crawlers), bad bots, and humans.

AI enables us to research a substantial amount of data and permits cybersecurity groups to evolve their strategy to a usually changing panorama.

“By looking at behavioural patterns, companies will get answers to the questions ‘what does a mean consumer journey look like’ and ‘what does an unstable uncommon adventure look like’. From here, we are able to unpick the cause in their internet site visitors, getting and staying beforehand of the awful bots,” explains Mark Greenwood, chief Technical Architect & Head of information technology at Natalia.

4.3 Breach Risk Prediction

AI systems help determine the IT asset stock that's a correct and designated record of all devices, users, and programs with special tiers of access to various systems.

Now, considering the asset inventory and risk publicity (as discussed above), AI-based totally structures can predict how and where you're most probably to be compromised so you can plan and allocate assets toward regions of maximum vulnerabilities.

Prescriptive insights from AI-based evaluation permit you to configure and improve controls and tactics to boost your cyber resilience.

4.4 Better Endpoint Protection

The number of devices used for working remotely is fast growing, and AI has an important role to play in securing all the ones endpoints.

Certain, antivirus answers and VPNs can assist in opposition to far off malware and ransomware attacks, however they frequently work primarily based on signatures.

This means that with a view to live protected towards the today's threats, it turns into essential to keep up with signature definitions.

This will be a challenge if virus definitions lag behind, both because of a failure to update the antivirus solution or a lack of awareness from the software program seller. So if a new kind of malware assault takes place, signature safety may not be capable of protect towards it.

“AI-driven endpoint safety takes a different tack, by way of setting up a baseline of behaviour for the endpoint thru a repeated training method. If something out of the regular happens, AI can flag it and take movement — whether that’s sending a notification to a technician or maybe reverting to a secure kingdom after a ransomware assault

.

This provides proactive protection against threats, rather than waiting for signature updates,” explains Tim Brown, vice chairman of security architecture at Solar Winds.

CHAPTER 5

NETWORK SECURITY THREATS AI SOLUTIONS

5.1 Malware Solution

Malware is that the malicious code that affects the computer system directly or indirectly out of that ‘94% of all malicious executables are polymorphic’ as declared during an analysis by Webroot 2018. The polymorphic malware mechanically re-codes itself anytime it propagates or is distributed. A large quantity of malware detection technology relies on signatures or heuristics. The signature detection engines find precisely the piece of malware that is a similar, despite what changes around it. This system helps to spot many alternative variants of malware. Also, a few of them area unit area unit mistreatment heuristics detection engines because of it got to acquire several resources cannot be used on a large scale.

5.2 Ransomware Solution

Some analysis students at the University of Kent revealed the paper concerning a prophetic model named Ran deep that is a machine learning-based model providing info on finding and identifying behavioural patterns for improved ransomware detection and response of 18 families of ransomware.

5.3 DDoS Attack Solutions

There are unit loads of ways developing to counter DDoS attacks like signature or anomaly-based detection, network intrusion detection tool-SNORT, and plenty of alternative techniques separating legitimate and malicious traffic. If the traffic is simply too huge then the distributed computing can be used.

a) VERSIVE
b) LOGRHYTHM
c) DARKTRACE
d) SPARKCOGNITION
e) SHAPE
f) CHECK POINT
g) CROWDSTRIKE
h) CYBEREASON
i) PERIMETERX
j) OBSIDIAN

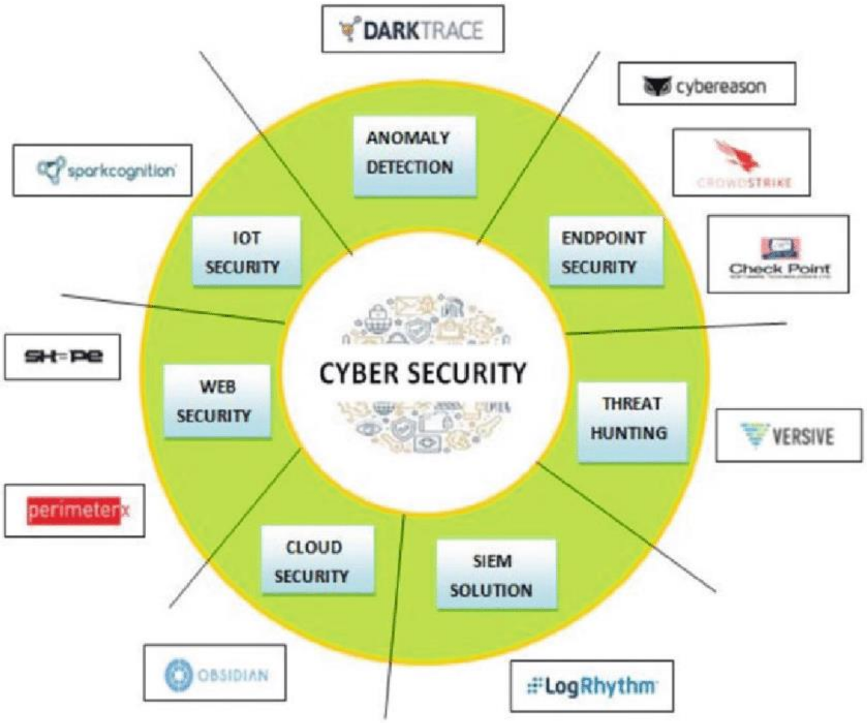


Fig-5.1 Emerging Security Start-ups Based On AI

5.4 IOT-Related Treats Solution

Several corporations like Cisco, Hitachi, Huawei, etc., square measure all developing their resolution product with completely different approaches. Securing IOT devices desires each protection and privacy at the network and service supplier level. For this, a DDoS detection methodology exploitation ANN is used for IOT networks. This system relies on the categorization of legitimate and offensive patterns. The planned system is simulated and tested to obtain quite 99% detection accuracy. Also, making and implementing some policies which will see to the lifecycle challenges of the IOT device regarding their privacy and security.

5.5 Phishing Solution

Putting in place correct access management is important, that is, employees with thorough understanding ought to lean access to accounts accordingly. Also, with the increasing trend of AI and machine learning companies square measure developing with new phishing detection models to improve business.

5.6 Man-in-the-middle Attack Solution

The foremost common methodology to control MITM is SSL/TLS encoding protocols; this methodology uses a key that is encrypted and decrypted at the sender and receiver ends, severally. But the hacker cans still find out the communication between the two by knowing the sender and receiver themselves as they use sure third parties which can be not authentic. Therefore, rather than one third party, multiple communication channels started getting used. The new manner that came into look is by employing a virtual private network (VPN). It encrypts the user's web association to disguise it from the hackers, although it's intercepted, there's decryption. Also, the internet speed isn't affected.

5.7 SQL Injection Solution

Numerous resolution to unravel SQL injection square measure currently based on machine learning and AI, one amongst the analysis papers by a student of Sanjose University conferred one amongst one amongst ways that to unravel this threat. In that, Gradient Boosting Classifier methodology is employed to classify the incoming truckling with a mixture of parameters. Exploitation this formula, the accuracy of getting desired solutions improved to 97.4%. Despite this, different network neural techniques may be accustomed scale back SQL injection attacks.

CHAPTER 6

CONCLUSION

AI is quick rising as vital technology for enhancing the performance of IT security groups. Humans will not scale to sufficiently secure associate enterprise-level attack surface, and AI offers the much-needed analysis and threat identification that may be utilized by security professionals to attenuate breach risk and enhance security posture.

Moreover, AI will facilitate discover and prioritise risks, direct incident response, and establish malware attacks before they are available into the image.

So, even with the potential downsides, AI can serve to drive Network Security forward and facilitate organizations produce a lot of strong security posture.

In recent years, AI has emerged as required technology for augmenting the efforts of human information security teams. Since humans can no longer scale to adequately protect the dynamic enterprise attack surface, AI provides much needed analysis and threat identification that can be acted upon by cybersecurity professionals to reduce breach risk and improve security posture. In security, AI can identify and prioritize risk, instantly spot any malware on a network, guide incident response, and detect intrusions before they start.

AI allows Network Security teams to form powerful human-machine partnerships that push the boundaries of our knowledge, enrich our lives, and drive Network Security in a way that seems greater than the sum of its parts

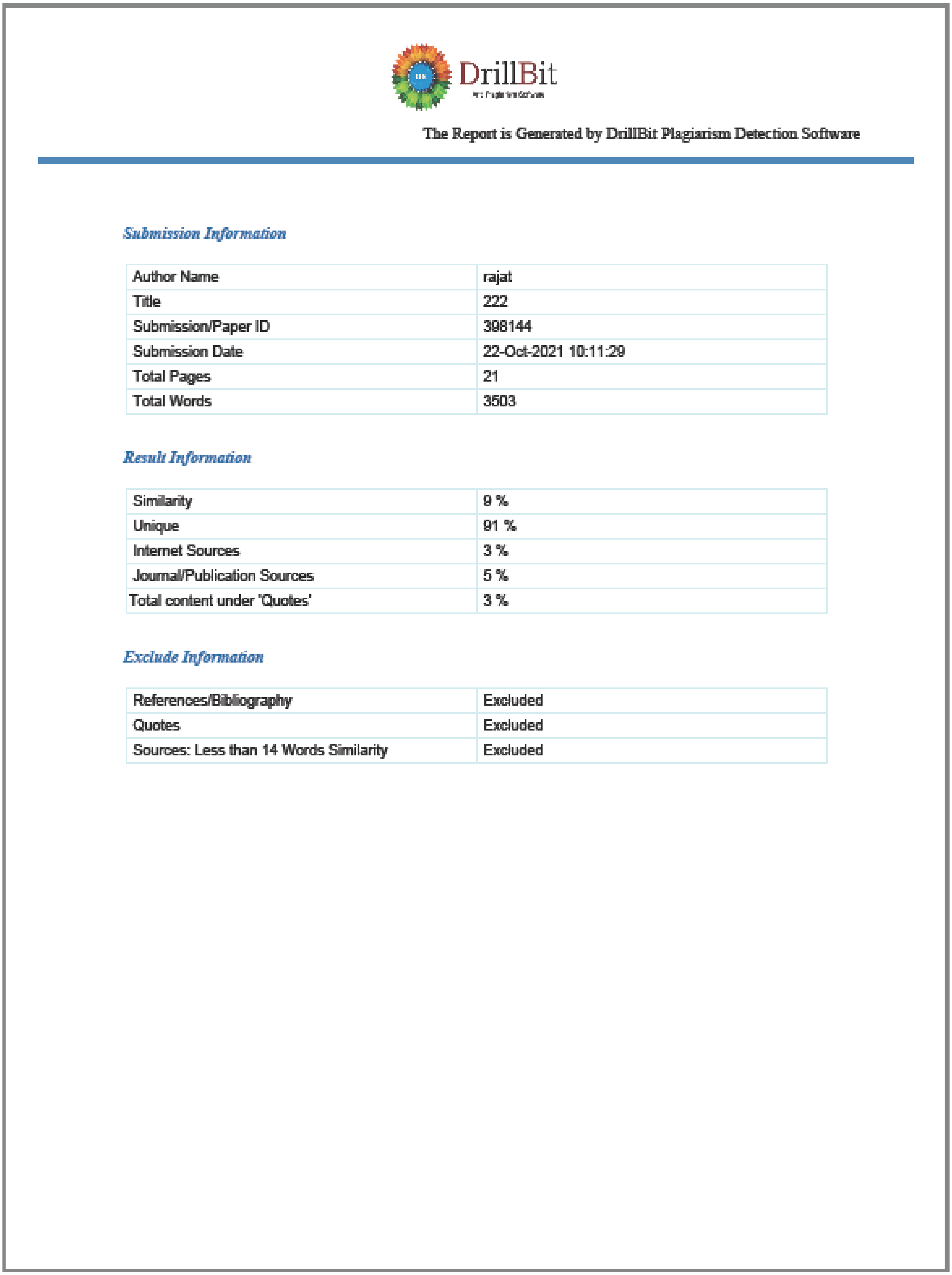
.

REFERENCES/BIBLIOGRAPHY

1. Suchita Gupta, Emerging role of AI in network security, October 2021.
2. https://www.paloaltonetworks.com/cyberpedia/network-security.
3. Nilam Choudhury, past to future of network security, Advances in Intelligent Systems and Computing, October 2020, DOI: 10.1007/978-981-15-6014-9_43.
4. https://www.a10networks.com/blog/5-most-famous-ddos-attacks
5. https://www.avast.com/en-in/business/resources/future-of-network-security#mac.
6. https://www.cm-alliance.com/cybersecurity-blog/8-benefits-of-using-ai-for-cybersecurity

BOOK

1. CEPS-TFR-Artificial-Intelligence-and-Cybersecurity by Lorenzo Pupillo, Stefano Fantin Afonso Ferreira, Carolina Polito, May 2021.
2. AI & ml in cybersecurity, Raffael Marty, August 2018.
3. Role of AI in Network Security, December 2019.
4. Software defined networking and security by Dijing Huang, Ankur ET.AL March 30.



The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	rajat
Title	222
Submission/Paper ID	398144
Submission Date	22-Oct-2021 10:11:29
Total Pages	21
Total Words	3503

Result Information

Similarity	9 %
Unique	91 %
Internet Sources	3 %
Journal/Publication Sources	5 %
Total content under 'Quotes'	3 %

Exclude Information

References/Bibliography	Excluded
Quotes	Excluded
Sources: Less than 14 Words Similarity	Excluded