iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** X **Month of publication:** October 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.47183

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue X Oct 2022- Available at www.ijraset.com*

# A Study of Cyber Security Challenges and Developing Tendencies in the Latest Technologies

Chetan Vijaykumar Dalave[1], Anushka Alok Lodh[2], Tushar Vijaykumar Dalave[3]
[1, 2]*Dept.Of Computer Engineering Savitribai Phule Pune University, RMD Sinhgad College of Engineering Pune, Maharashtra, India*
[3]*Dept.Of Information Technology Engineering Savitribai Phule Pune University, of Engineering Pune, Maharashtra, India*

***Abstract:*** ***Today, with modern lifestyles, people have become involved in the life and use of technology. More technology for financial transactions as well as shopping in their cyberspace.At the same time, the protection of knowledge has become increasingly difficult. In addition, the proliferation of social media has led to an increase in online crime or cybercrime. in the world data security plays an important role in information technology. Information with security become one of the major challenges of today. Whenever we think of cybersecurity, we come first think of the 'cybercrimes' that are spreading every day. Different governments and Businesses take various steps to avoid this form of cybercrime. In addition to numerous cyber security measures, many people are also very worried about it. This paper focuses primarily on cybersecurity concerns related to new technology. It also focuses on the new. Cybersecurity, ethics, and technologies for development that affect cybersecurity.***
***Keywords: Cyber security and cyber crime, cyber ethics, social media, cloud computing, android apps etc.***

## I. INTRODUCTION

Nowadays people can able to send and receive any form of data can be email or audio or video. With the click of a button, but did he ever? Think about how securely its data ID is being transferred. Or sent to another person safely without anyone. Disclosure of information ??? The answer lies in this Cyber Security. Today the Internet is the fastest. Infrastructure is growing in everyday life. Today's technical environment is very up-to-date technology is changing the face of man. By the way, because of these emerging technologies, we are unable to protect our privacy. Very effective information and therefore Cybercrime is on the rise these days. More than 60% today Commercial transactions are done online, so this High-quality security is required for the field. Transparent and excellent transactions. So cyber security has become a recent issue. The scope of Cyber security is not limited to security. Information in the IT industry, even different other sectors like cyberspace, etc.

Even the new technologies like cloud computing, mobile computing, e-commerce, net Banking, etc also require a high level of security. Because these technologies are important information about a individual's person safety has become a necessary thing. Promoting cyber Protection and security of important information Infrastructure is essential for every country. Security and economic well-being to create the Internet are secure (and protects Internet users). Must be for new development Services as well as government policy. The fight against cybercrime is needed. Comprehensive and secure method. Take it technical measures alone cannot stop anyone Crime is important to law enforcement. Agencies are allowed to investigate and take effective action against cybercrime. Many today Nations and governments are working hard. Lawson Cyber Securities to Prevent Loss of some important information. Everyone Individuals should also be trained in this cyber. Protect and protect yourself from the rising cybercrime.

1) *Cyber Crime:* Cybercrime is a term for a crime that uses a PC for robbery and commission of a crime. United The State Department of Justice has extended the scope of cybercrime to cover any crime that an Evidence storage tool. The growing list of cybercrimes includes computer crimes. Network interference and the spread of PC viruses, as well as computer-based variety Crimes such as theft, stalking, intimidation, and coercion. Most of the cyber crimes in the common people Language can also be defined as crimes committed using PCs and the web to steal or sell identities. A person who is involved in trafficking or stalking or disrupting operations with a malicious program. Because technology plays a vital role in a person's daily life, cybercrime can happen. Increase with technological advancement.
2) *Cyber Security:* Privacy and information protection can be basic security concerns that any company cares about constantly. We currently prefer square measurement in highly digital or cyber specific. The environment in which all data is stored. Social networking sites provide an environment wherever possible. Consumers feel safe working with their friends and family, and cyber criminals want to steal. Personal information through social media sites.

3) *Scope of The Study:* The interactive structure of the financial environment will have a direct impact on one aspect. Institutional infrastructure and the sensitivity of the financial sector to cybercrime, in particular attacks on denial of services. To keep all confidential information from falling into the wrong hands, the finance sector must constantly track and innovate its systems. Banking Sector has always been and continues to be a leading player in enforcing security systems and behavior leading the Cyber Security investment division.

## II. GOALS OF CYBER SECURITY

The ultimate goal of cybersecurity protect stolen or collaborative data to achieve this we focus on 3 main goals of cyber Security.

1) Defensive the Privacy of Information.
2) Conserving the Integrity of Information.
3) Controlling the Obtainability of information only to approved users.

These purposes practice privacy, Integrity, and availability (CIA) triad, the basis of the whole safety Agenda this CIA Triad model is a safety one model aimed at guiding strategies for data security within the premises of society or corporation. This model is mentioned in a similar place. AIC (Availability, Integrity, and Privacy) to try to sidestep errors Central Intelligence Agency. In introductory remarks, the triads reflect the three most important safety mechanisms. The CIA standards are the same. The greatest exercise of societies and businesses once they add a new application, one does. Record or guarantee access until information. To be completely safe from data, all these should result in safer areas. These are safety strategies that do their best together, and therefore monitoring it can be wrong a policy. The CIA Triad is the highest collective standard. Measurement, selection, and proper safety of tools risk reduction panels.

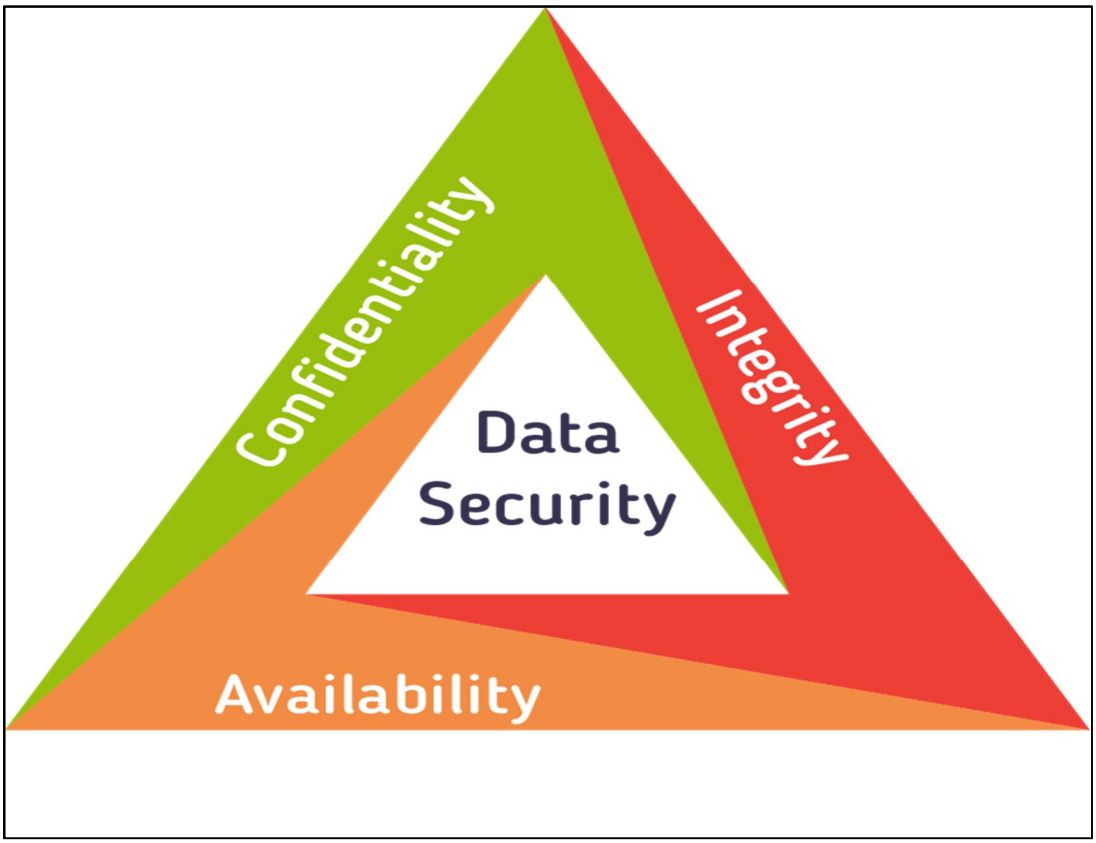



Fig.1: CIA Trails

a) *Confidentiality:* Guarantee that your complex Statistics can reach recognized users and Safety No information is disclosed Unintentionally. In that case, your key is private and desired. The power adventures that can't be shared Ultimately prevent privacy.

Methods to safeguard Confidentiality:

- Data encryption

- Two or Multifactor verification
- Confirming Biometrics

*b) Integrity:* Make sure all your data is correct. Reliable and it should not be replaced with one in the show the other reality. Integrity ensures methods:

- There will be no entry to delete any illegal records, which also breaks privacy.
- Operator Contact Controls.
- Need to be able to get proper backup.
- Version Supervisor must be close to checking login that has changed.

*c) Availability:* Each time the operator has made a request there will be no resources for one part of the data notice of any dispute such as denial of service (DoS). Must be able to get complete proof. for example, if a website is in the hands of an attacker DoS interferes with this ability to get.

## III. TRENDS CHANGING CYBER SECURITY

Below are some trends that are having a huge impact on cyber security.

1) *Web Servers:* Risk of attacks on web applications Extracting data or distributing malicious code the cybercriminals distribute them. Malicious code through legitimate web servers they have compromised. But data theft attacks, most of which get media attention also a big risk. Now, we have a great need for emphasis on web servers and web security applications web servers are especially good. A platform to steal these cyber criminals data should therefore always be used securely browser especially during important transactions so that they do not fall victim to these crimes.
2) *Cloud Computing And Its Services:* These days all small, medium, and large companies are slowly adopting cloud services. In other words, the world is moving slowly towards the clouds. It presents the latest trend on the biggest challenge for cyber security, as can traffic. Go around the traditional points of inspection. Furthermore, as the number of requests available in Cloud Groves, for policy control will also do web applications and cloud services. Need to be prepared to prevent damage to valuable information. Although there are cloud services. Developing their own model still has a lot of problems their security is being raised the cloud can give a lot of opportunities but it always remembers that as the cloud forms to increase its security concerns.
3) *APT's And Targeted Attacks:* APT stands for (Advanced Persistent Threat) which is a completely new level of cybercrime. For years Network security capabilities such as web Filtering or IPS have played a key role. Identifying such targeted attacks (mostly later) Initial Compromise). As the attackers grow using more daring and more confusing techniques, Network security needs to be integrated with security services to detect attacks. So we have to improve our security techniques in order to prevent further threats in the future.
4) *Mobile Networks:* Today we are able to connect with anyone part of the world but for these mobile networks security is a big concern. These days there are firewalls and other security measures. Being insecure because people are using devices such as a tablet, phones, PC, etc. In addition, securities are required to be used in applications we should always think about their security issues on mobile networks. There are more mobile networks victims of these cyber crimes take great care. These should be taken in case of security issues.
5) *IPv6: New Internet Protocol:* IPV6 is the new Internet Protocol that is replacing IPv4 (older version), which contains it is usually the backbone of our networks. Massive Internet IPv6 protection is not the only question to port IPv4 capabilities. While IPv6 is a wholesale alternative to making more. IP addresses are available, and many more. Fundamental changes to the protocol are needed to consider security policy. That's why it's always a good idea to switch to IPv6. It is can able to reduce the risks associated with Cybercrime.
6) *Encryption of the code:* Encryption is the process of encoding messages (Or information) in a way Listeners or hackers can't read them Encryption scheme, messages, or information is encrypted using an encryption algorithm, and convert into unreadable ciphertext. It can only be done with the use of an encryption key. Encryption at the most basic level protects data privacy and integrity. But more the use of encryption brings more challenges to cyber security. Encryption is also used for security. Data in transit, for example, data transmitted via networks (eg Internet, e-commerce), mobile telephone, and wireless microphone, wireless intercom, etc. Encrypting the code lets anyone know if there is one information leakage.

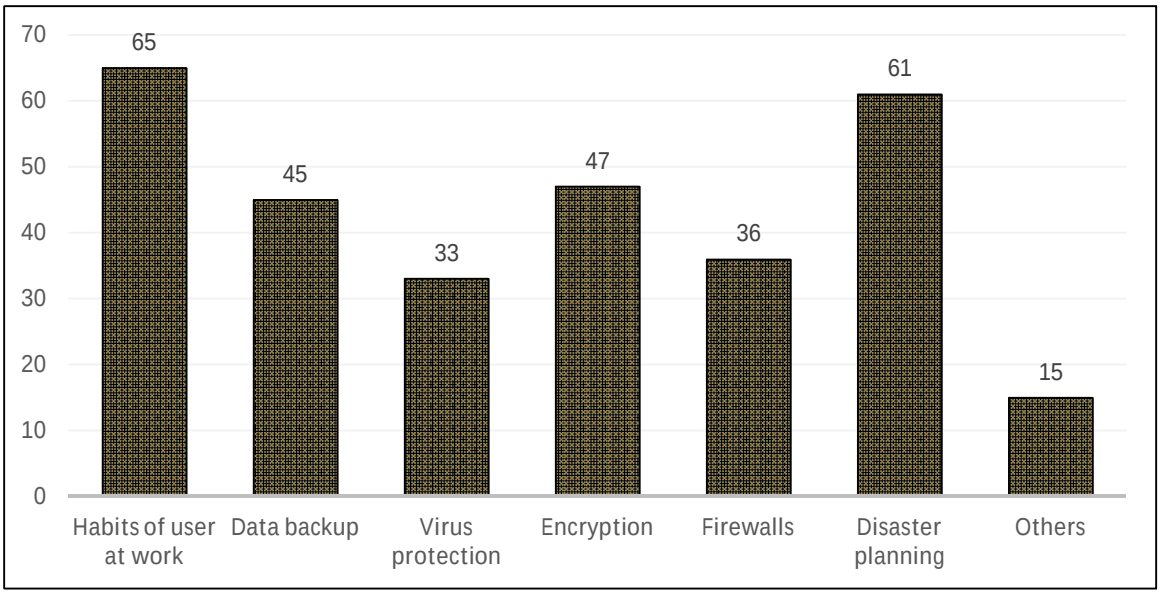



Fig.2: The chart above shows the major threats to networks and cybersecurity

## IV. SPECIFIC CYBER SECURITY TECHNOLOGIES

1) *Access Control and Identity Management:* Username / Password Collection Initially the basics of computer access control from in the year 1960.
2) *Authentication of data:* The documents we receive should always be this is to be verified before downloading it should be checked whether it is from the beginning. Reliable and trustworthy sources have not changed. Verification of these documents is usually done with existing antivirus software on devices. This is good anti-virus software it is also important to protect the device from viruses.
3) *Malware Scanners:* This is the software that usually scans all the files. And for documents in the system Malicious code or harmful viruses. Viruses, Insects, and Trojans are examples of horses. Malicious software that is often grouped is also known as malware**.**
4) *Firewalls:* A firewall is a software program or piece of hardware that helps hackers screen out viruses and the bugs that try to reach your computer internet all messages entering or leaving the Internet pass through existing firewalls, which check every message and block them. Which do not meet certain security standards. That's why firewalls play an important role in malware detection.
5) *Anti-virus software:* Anti-virus software is a computer program. Detects, intercepts, and acts to disarm. Remove malicious software programs, e.g. Viruses and worms. Most anti-virus programs add an auto-update feature that enables programs to download new virus profiles it may soon be testing new viruses they are being discovered. Is an anti-virus software essential and basic requirement for every system.

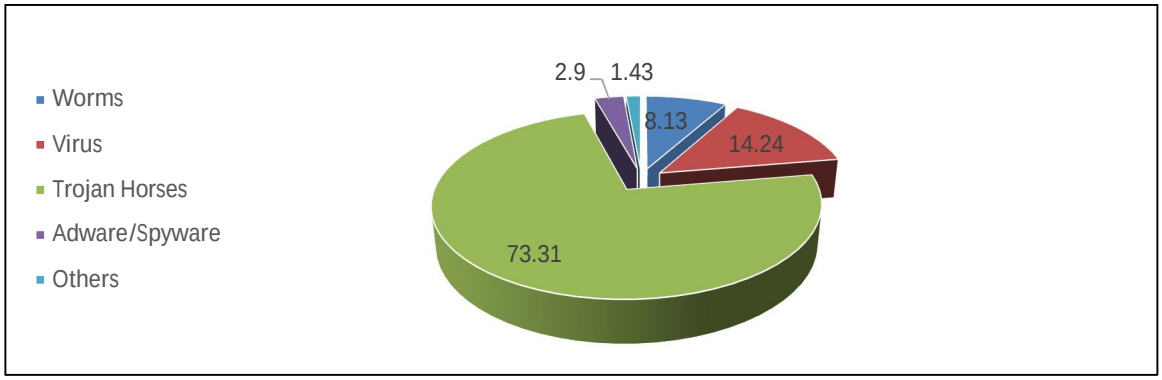


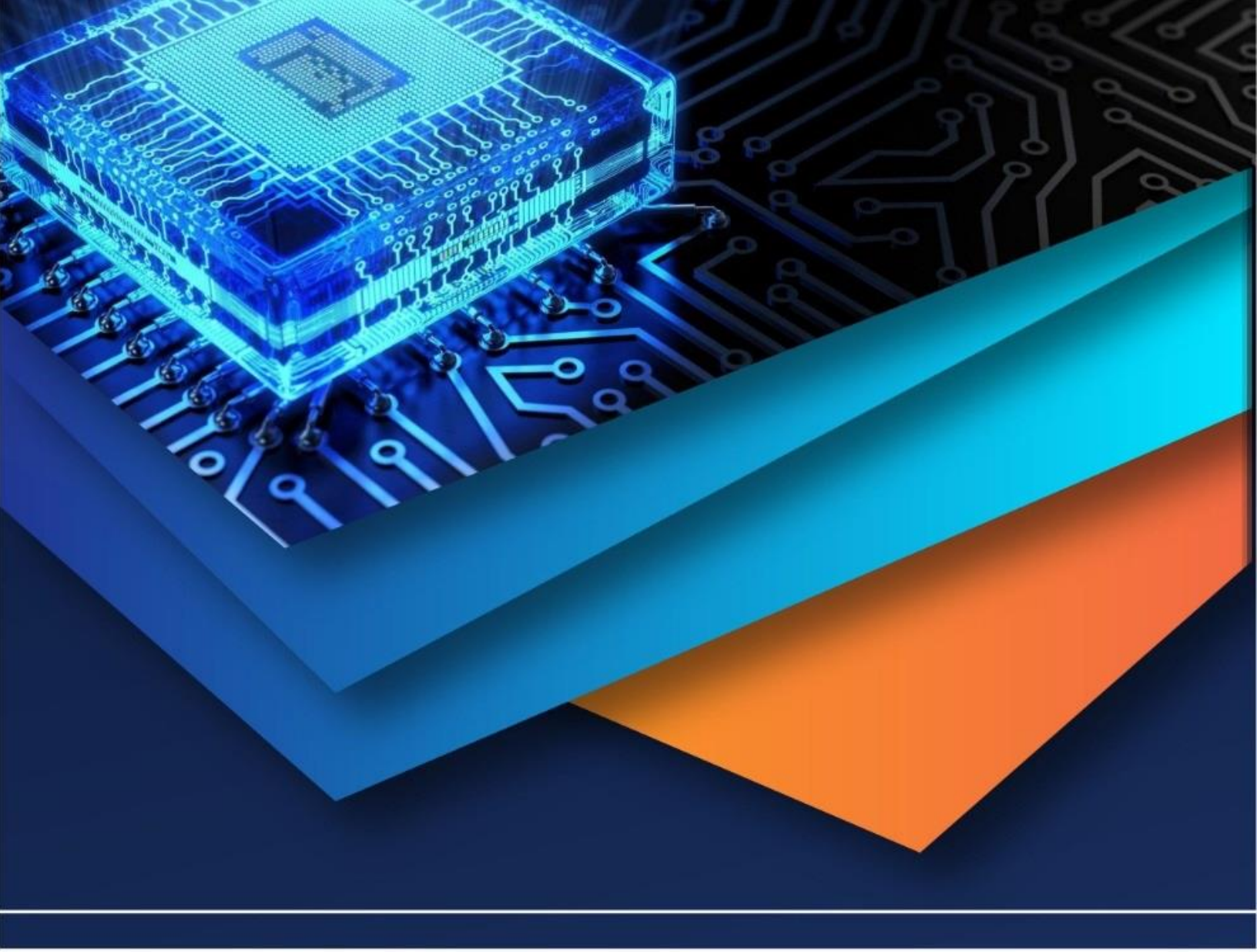

Fig.3: Percentage of Malware Attacks.

## V. CONCLUSION

Computer security is a broad topic more important in the world and is highly integrated with networks used to perform important transactions. Cybercrime continues with each passing year the paths that pass and so on protect information with the latest and disruptive technologies, with new one's cyber tools and threats that everyone faces. Days, not just with organizations challenging how do they protect their infrastructure, but how? They need new platforms and intelligence doing so is not the best solution for cybercrime but we must do our best. Minimize them to keep them safe and secure future in cyberspace.

## REFERENCES

[1] Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India
[2] VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018
[3] Yang, Miao, "ACM International Conference Proceeding Series", vol. 113
[4] Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011
[5] https://cltc.berkeley.edu/scenario-back-matter/
[6] Cyber Security Strategy of United Kingdom, 2009
[7] ITU Cyber Security Work Program to Assist Development Countries, 2009
[8] Rev. Jonames Burg, TTU WTSA Resolution 50, 2008
[9] ITU Cyber Security Work Program to Assist Development Countries, 2008
[10] Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2
[11] Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012
[12] Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016
[13] VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018
[14] https://www.getgds.com/resources/blog/cybersecurity/6-cybersecurity-threats-to-watch-out-for-in-2021
[15] ] Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019
[16] MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand
[17] Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15
[18] J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162, 2015
[19] Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. Comput.Secur. 2017, 70, 199–223
[20] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY