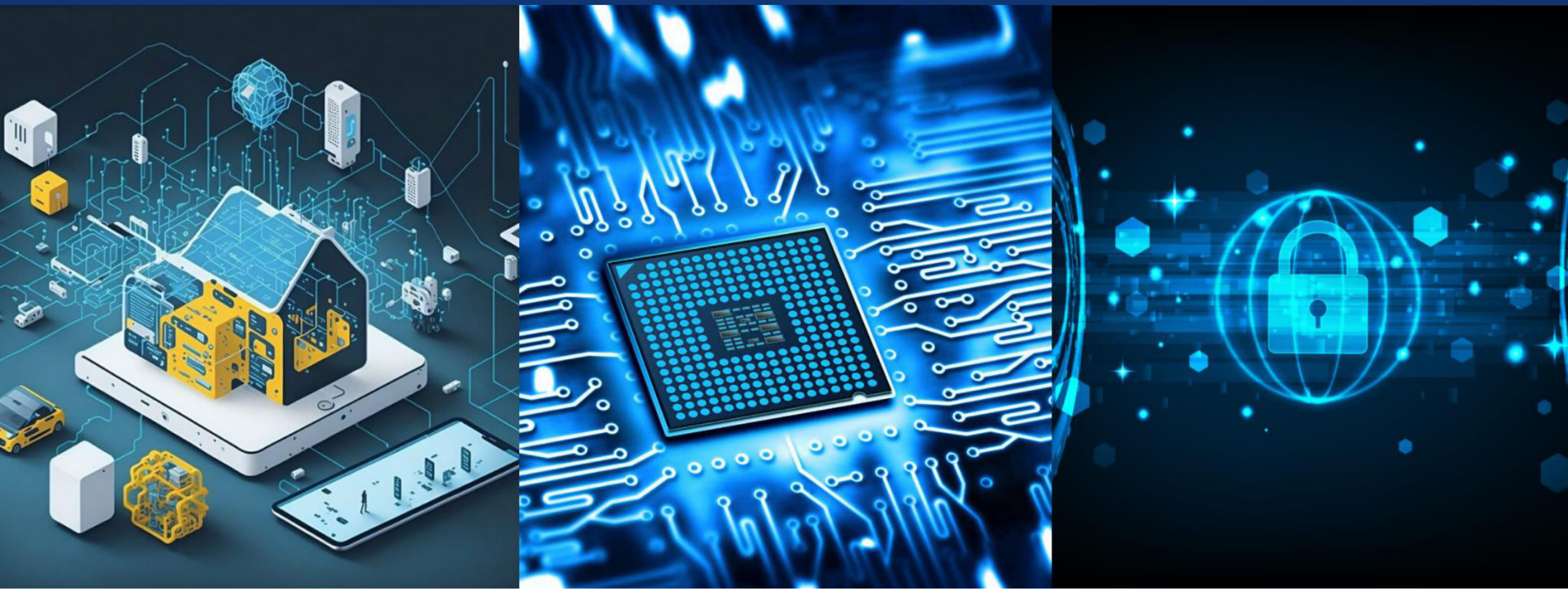
IJIRCCE

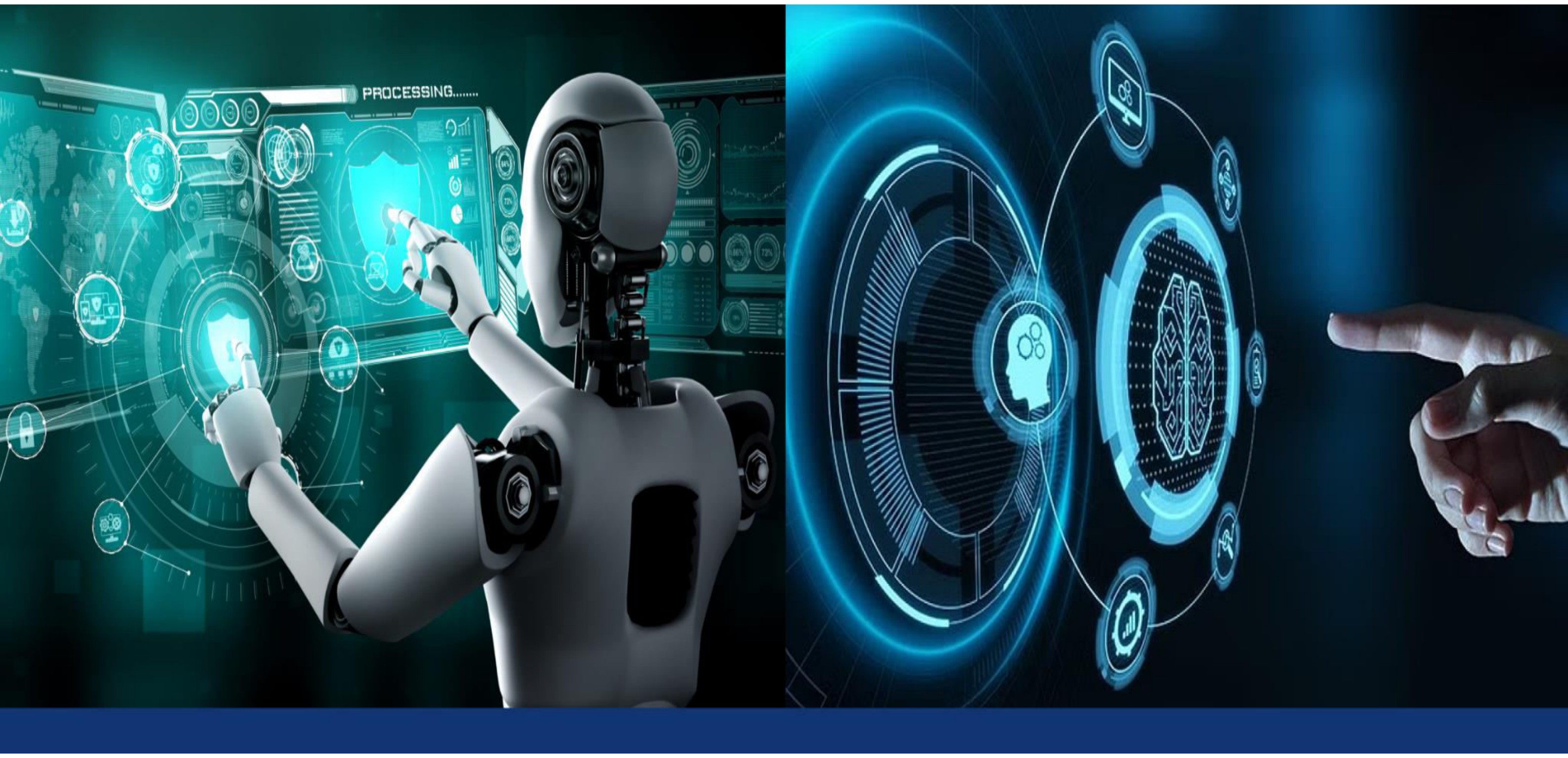
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Highly Sophisticated AI/ML Technology Based Cyber Security Attacks: AI/Finance Sectors to Face Major Threats

Dasaka VSS Subrahmanyam[1], Vanama Bhavani[2], M.A. Aziz Siddiqui[3], Kantale Vishwambari[4]

Professor, Department of CSE, Keshav Memorial Engineering College, Hyderabad, Telangana, India[1]

Assistant Professor, Department of CSM, Keshav Memorial Engineering College, Hyderabad, Telangana, India[2]

Assistant Professor, Department of CSE, Keshav Memorial Engineering College, Hyderabad, Telangana, India[3]

Assistant Professor, Department of CSE, Keshav Memorial Engineering College, Hyderabad, Telangana, India[4]

ABSTRACT: AI/ML technology is being misused to design and develop highly sophisticated phishing campaigns to make advanced cyber-attacks on Banking/Financial sectors. Cyber attackers always mining for new innovative methods to attack innocent public/customers. Their modern tools have been creating hindrances to provide cyber-attack free services to financial/banking and to all other major sectors. They have been utilizing AI/ML technology and its tools to reattack on AI itself by means of various ways. Prominent measures are necessitated to detect, arrest and eradicate their existence in the nip of the bud.

KEYWORDS: AI/ML Technology, Cyber Security Attacks, Mule Accounts, Phishing Campaigns, Spam Calls

I. INTRODUCTION

According to the Telangana Cyber Threat Report 2025, numerous cyber threats, as a result of advanced and emerging AI/ML technologies, have been taking place in cyber-crimes. New AI/ML technologies help in the evolution of new Ransomware/Malware attacks. Cyber criminals are able to make cyber-attacks every time with more sophisticated methods because of the new emerging technologies. These cyber-attacks are forecasted on areas such as AI/ML technology, infrastructure, financial/banking sector, insurance sector and many other prominent sectors. The Report indicates that an AI driven deepfake technology and personalised vector attacks are being used by cyber criminals. These kinds of attacks are very harder to detect.

Moreover, an AI/ML driven ransomware/malware will adapt in real-time environments, of any kind of system, very easily to evade additional security measures/tests, of the concerned environments. This mechanism will make all data to compromise with malicious software, which is injected by the ransomware/malware. It makes all system environments to lose their security and integrity, which is a very serious threat to all kinds of domains/sectors. The same serious threat can be affected to critical AI systems and their applications, healthcare sectors, autonomous Transport systems and so on. They may target on any system for ransom and to disrupt the national integrity, as a whole.

AI/ML driven ransomware/malware always focuses on detecting system vulnerabilities and using new strategies in finding flaws in users' behaviour. It has become a new challenge to detect and prevent these kinds of strategic and technology driven attacks for traditional security systems. Traditional security systems do not embed with the latest technology driven strategies to face them. Unlike traditional security systems, AI/ML driven ransomware/malware systems are highly dynamic. It is clear that, in the near future, ransomware/malware attacks will further advance beyond simple encryption and decryption mechanisms. Cyber criminals will accelerate their extortion tactics that involve data theft and threats to release sensitive data in public domain for ransom. Additionally, they may target critical infrastructure sectors like defence, energy, transportation and healthcare, by detecting vulnerabilities in their operational mechanisms, and Industrial IoT (IIoT) to cause physical damage, disruption, sabotage and collapsing the entire infrastructure. Cyber criminals may even dupe and threat their trusted vendors. They may concentrate on open-source vulnerabilities to inject their malicious software, like Solar Winds incident. Once an open-source software is inflicted by malicious code, every user of that software will become preys to cyber criminals. In this way, they have been trying to spread their wings at large over general public/customers of any sector. The reliance on third party services will heighten the risk and envisaging enhanced supply chain security measures.

II. SPAM CALLS: A MAJOR THREAT

Spam calls and messages refer to unrequested communications committed by fraudsters for fraudulent or marketing purposes. They target a large number of mobile users. A spam message generally an unwanted and irrelevant bulk message. It is used for advertising of newly launched products. Now they are being used by cyber attackers for phishing or spreading ransomware. These messages can be in the form of emails, text messages, or appear in social media or by means of phone calls. They are very harmful to systems, if they contain malicious code. These are sent by scammers or by bots. Cyber criminals use it as their main platform for attacking mobile users for ransom.

Department of Telecommunications, a Government of India’s Organization, says that around 60% of Indians receive at least three spam calls a day, compared to the daily global average of 105 spam calls. Illegally acquired SIM cards are being used by scammers across the country. As per the report, at present, there are 134 crore mobile connections (officially registered mobile numbers), (as per the instructions of the Department of Telecommunications), in India and among them nearly 79.42 lakh fraudulent SIMs were detected. After a strict reverification, among the 79.42 lakh fraudulent SIMs, 73.14 lakh SIM connections were disconnected immediately. And 70,895 SIMs were Blacklisted. A major fraud was unearthed where a single offender procured 6,800 SIMs by using other persons’ photographs. Conduction of strict and thorough verification makes a concrete path to bring down various kinds of cyber-attacks.

Table 1: Statistics of Mobile Connections: a Report Given by the Department of Telecommunications in 2024

Total No. of SIM cards	Fraudulent SIMs	Disconnected SIMs after verifications	Blacklisted SIMs	A Major Fraud detected
134 crore	79.42 lakh	73.14 lakh	70,895	One person managed to get 6,800 SIMs

A recent study revealed that six out of ten persons receive at least three spam calls daily, while nine out of ten persons receive spam messages every day. These issues have impacted our Indian economy with financial losses due to cyber-attacks. Many have been originating from spam communications. They resulted in loss of nearly $ 113.3 billion. In India, strict regulations have been implementing by TRAI (Telecom Regulatory Authority of India), as a result, consumer spam complaints are decreased by 20%, from 1.8 lakh in August 2024 to 1.15 lakh in October 2024. These numbers will surely be increased in future.

According to India Cyber Threat Report 2025, up to 17% of organizations faced cyberthreats at least one in 2024 and about 9% attacks every week/month. Similarly, at least 1.5% of organizations experienced one cyber attack every 24 hours. While 13.2% of organizations faced business disruptions over the past 12 months due to cyberattacks. Among them 6.3% incurred financial losses due to online threats. The report says that at least 72.5% of organizations did not report any cyberattacks. Every organization has to report the authorities about the cyber threat they received. It will help the authorities to know the nature of attacks in different modes and they will be able to take appropriate actions upon cyber criminals. It also helps organizations to protect themselves from the malicious activities of cyber criminals.

These attacks include phishing, vishing, smishing, shoulder surfing and ransomware/malware attacks. AI/ML based attacks were new kind of cyberattacks in 2024 along with software vulnerabilities. Nearly 69% of organizations reported that they did not suffer any impact from cyberattacks. But the magnitude of the impact of AI/ML based phishing threats has been more comparing to the previous versions of cyberattacks. Traditional cyber security software has to undergo major modifications accordingly. They have to incorporate AI/ML based software updates from time to time. Traditional software has to be strengthened in such a way that it has to detect, arrest and eliminate all kinds of malware include viruses, spyware, worms, Trojan viruses, adware and ransomware.

III. CYBER CRIMINALS: FOCUSED ON TELANGANA STATE

Cyber criminals are operating through Telegram-based Group targeted various key sectors in Telangana state. Their aim is to breach data and disrupting all regular operations frequently. A significant incident, attack by the Telegram-based Group “Black Code”, taken place on February 19, 2024, which leaked more confidential information from the Telangana Government portal (data.telangana.gov.in). Another attack was taken place by “Nusantara” on February 21, 2024, on SC/ST Commission portal (scstcommission.telangana.gov.in). Another significant attack was targeted on Mr Mallu Bhatti Vikramarka’s website, who is a Deputy Chief Minister of Telangana State, on March 2, 2024. Another cyber criminals’ group “Z-BLACX-H4T” leaked credentials of the Telangana Government’s official portal (telangana.gov.in).

A cybersecurity company “Garuda Security” protected the website of jnafau.ac.in from cybercriminals . “Bangladesh Dark Net Hacker Boys” launched a DDoS attack on www.uohyd.ac.in and many others. Cyber attacks were even taken place on private organizations too. Sri Sathya Sai Seva Organization was attacked by a malware, where attackers put public sensitive government documents, citizens’ data and some other important communications on public domains. Another major cyberattack, was taken place on one of Asia’s largest educational group, targeted its hospitals and educational services, disrupting patient care and administrative operations, for a big ransom.

Table 2: Cyberattacks on Telangana websites in 2024

S. No.	Ransom Group	Date of attack	Attacks on websites of
1	Black-Code	February 19, 2024	data.telangana.gov.in
2	Nusantara	February 21, 2024	scstcommission.telangana.gov.in
3	Ransomware attack	March 2, 2024	Dy. CM of Telangana State
4	Z-BLACX-H4T	March 6, 2024	telangana.gov.in
5	Ransomware attack	March 16, 2024	www.jnafau.ac.in
6	Bangladesh Dark Net Hacker Boys	2024	a DDoS attack on www.uohyd.ac.in
7	Sri Sathya Sai Seva Organization (a private organization)	September 19, 2024	Sri Sathya Sai Seva Organization

The following data revealed the range of cyberattacks taken place in Telangana state in 2024. All these attacks are of Ransomware/Malware.

Table 3: Ransomware/Malware attacks in Telangana State in 2024

Ransomware/ Malware	Average attacks	Attacks per Day	Highest Detections
Malware detections	62,52,023	17,128	Noticed in Q1 at 16,82,842
Ransomware detections	17,505	47	

Primarily, cyberattacks were focused on four major cities in Telangana state. Details of attacks are shown in the following table.

Table 4: Top Cyberattack affected Cities in Telangana State in 2024

S. No.	Name of the City	No. of Detections
1	Hyderabad	59,81,619
2	Khammam	52,518
3	Warangal	52,037
4	Nizamabad	28,049

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

According to the report, the threat environment in Telangana state is further complicated by a diverse range of attacks targeting primary sectors such as government, banking, financial services, health care, education, industries, manufacturing, insurance, and IT/ITES. It is transparent from the following statistics of the report.

Table 5: Sectors under cyberthreats in Telangana state in 2024

S. No.	Name of the Sector	No. of Cyberthreats / attacks happened
1	Government	3,62,255
2	Education	5,51,496
3	IT/ITES	1,15,552
4	Power & Energy	15,355
5	Telecom	8,641
6	Automobiles	1,90,625
7	Professional services	6,27,880
8	BFSI	27,837

IV. CYBERSECURITY PRACTICES TO BE ADOPTED

All organizations whether government/private sectors have to be more cautious about cyberattacks. All have to follow the proverb of “Prevention is better than cure”. All software employees have to be more aware of AI/ML driven highly sophisticated cyberattacks and their detection. It is the time to adopt the best cybersecurity practices, in general, in all software related organizations, whether big/small. The following measures are to be adopted:

- Using strong passwords for systems (using a minimum of 10-character length password which contains at least one character from each of the sets of small case letters, uppercase letters, numerals, and special characters. It is advised to use a password of length 15 characters containing all characters from the abovesaid sets. Periodic change of passwords is highly suggested.
- A multifactor/multilevel authentication (a 3-level authentication is safe) is strictly advised.
- Software updates are to be done on regular basis.
- Not to be clicked on unknown / suspicious links, as they may contain malicious code.
- Don’t prey to phishing emails. Delete emails which are from unknown URLs / unknown persons.
- Avoid / not entertain vishing calls (phishing voice calls).
- Report immediately to Cyber Security authorities, in case of receiving any cyberthreat call.
- Don’t answer to video calls from unknown mobile numbers.
- Ensure that you system is fully equipped with protective firewalls and anti-virus software.
- Don’t download any kind of free software from unknown websites. It is very harmful to systems. Download from authorized websites only.
- Don’t attend to suspicious text messages. Verify their authenticity.
- Network administrator has to make a periodical inspection of all systems.
- Don’t plug-in your mobiles / laptops / tablets / notebooks for recharge in public spaces.
- Cyber attackers make AI-based voice calls pretending that it is from your near and dear. So, don’t respond to them immediately unless verified personally.
- Avoid spam calls.
- Every software update is to be known to all employees of the organization.
- Organizations have to take care of data storage of valuable information in some other devices, which are not directly related to the system network. It will provide 100% safe to organizations even in case of severe cyberattacks taken place.
- Organizations are not to be compromised with the quality of their computer systems and other required software, all have to be purchased from the noted brand companies only. This will ensure the basic protection from cyber attackers.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. BASIC RECOMMENDATIONS

The following recommendations are necessitated among general public:

- Public awareness programs are to be conducted frequently.
- Banks have to educate its customers about cyber threats and attacks. They have to inform its customers about mule bank accounts. All customers are to be aware of spam calls / vishing calls / fraudulent text messages.
- Regulation of loan applications.
- Giving a clear information on usage of their Aadhar cards.
- Telecom Department has to conduct regular vigilance on SIM cards issue centers.
- Media has to participate in the campaigning of impacts of cybercrimes on public / economy / government.
- A minimum of 2-factor authentication is suggested.
- Immediate reporting mechanism is initiated by Government of India. Anyone can call 1930, In case of any kind of cybercrime / cyberattack.

VI. CONCLUSION

AI/ML driven highly sophisticated cyberattacks will dominate in near future and it is predicted that they grow in a non-linear mode. So, it is the time for Government, organizations, society as well as general public to be aware of and declare a technological war on all kinds of cyberthreats / cyberattacks, in order to protect our valuable information, hard earned money. Let us make our country a strong technologically driven nation in the world.

REFERENCES

English Newspapers:

1. The New Indian Express, Hyderabad Edition, The New Sunday Express, Magazine, Sunday, Page 1, February 16, 2025.
2. The New Indian Express, Hyderabad Edition, Thursday, Page 13, February 20, 2025.
3. The New Indian Express, Hyderabad Edition, The New Sunday Express, Magazine, Sunday, Page 3, March 30, 2025.

.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details