[1] **Sparsh Sopory**

[2] **Ruchit Rajneesh Tripathi**

[3] **Jaya Subalakshmi Ramamoorthi***

Impact of Cyberattacks During the COVID19 Pandemic and Beyond

Journal of Electrical Systems

Abstract: - The COVID-19 pandemic has drastically altered the global landscape, requiring both individuals and organisations to quickly adopt remote work and digital communications. The cyber threat landscape has changed as a result of this transformation, and cyberattacks—particularly ransomware attacks—have increased. In this study, the effect of cyberattacks on the COVID-19 pandemic is analysed, along with the consequences for the post-pandemic period. This study investigates the surge in ransomware attacks and the problems these attacks cause for individuals and organizations. The report offers beneficial insights for improving readiness and addressing the changing cyber threat scenario for politicians, organisations, and cybersecurity professionals.

Keywords: cybersecurity, ransomware, communications

I. INTRODUCTION

The unprecedented global disruption brought on by the COVID-19 pandemic has altered how people live, work, and interact with one another. Businesses and individuals increasingly rely on digital infrastructure and online platforms for their daily operations as remote work has become the norm [1,2]. However, this quick digital transformation has also given cybercriminals new opportunities to find weak points and loopholes to launch attacks, with ransomware attacks being especially prevalent [3]. The COVID -19 pandemic has prompted organizations to rapidly adopt remote workstations and leverage digital technologies [2], often without taking adequate cybersecurity measures [4]. Cybercriminals have taken advantage of this digital transformation and exploited vulnerabilities for ransomware attacks, in which malicious actors encrypt critical data and demand a ransom for its release [5]. This research is important for understanding the impact of cyberattacks, particularly ransomware attacks, during the COVID -19 pandemic and beyond. By examining the consequences faced by organizations and individuals, policymakers, businesses, and cybersecurity professionals can develop strategies to effectively mitigate these threats. In addition, the findings from this research will help prepare for future post-pandemic cybersecurity challenges.

1.1 Research Objectives and Methodology

The research paper includes a systematic review of existing literature, reports, and case studies on ransomware attacks during the pandemic COVID-19. Statistical data and expert opinions from cybersecurity professionals are included to provide a holistic perspective on the research topic. This research will also consider the post-pandemic period and incorporate predictive analysis to address future cyber threats.

This research examines the impact of ransomware attacks during the COVID-19 pandemic and beyond, contributing to the collective understanding of cybersecurity challenges. [4]. The results will help policymakers develop robust cybersecurity policies, assist organizations in improving their defences, and help individuals adopt best practices to protect themselves from cyberthreats.

1.2 Examine the elements influencing the rise in ransomware attacks during the COVID - 19 pandemic.

Due to the COVID-19 pandemic's forced remote employment of millions of experts globally, hackers now have a broad range of options [6]. In a recent global survey, 48% of respondents from the United States who worked from home reported receiving calls, phishing emails or texts in the previous six months, according to SailPoint Technologies Holdings, Inc.,

According to Juliette Rizkallah, CMO of SailPoint, "In the case of phishing, hackers target employees with malicious links embedded in carefully crafted emails." When employees click those emails, they unintentionally

[1] Student, School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore 632014, India. sparsh.sopory2021@vitstudent.ac.in

[2] Student, School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore 632014, India. ruchit.rajneesh2021@vitstudent.ac.in

[3] Assistant Professor Sr. Grade 1, School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore 632014, India.

* Corresponding Author Email: jayasubalakshmi.r@vit.ac.in

download keylogging software onto their PC, giving their login information to nefarious individuals. Once this happens, hackers can easily access crucial business assets and data while posing as a real employee. Identity security enables the quick identification and correction of suspected user behaviour anomalies, such as large data downloads or after-hours activity, by asking users to change their passwords or blocking access until anomalies are examined and addressed.

Phishing Attacks on remote workers are increasing for a number of reasons [4-6]. Half of employees in EMEA (Europe, Middle East, and Africa) and ANZ (Australia, New Zealand), as well as one in three Americans, work remotely using their own personal devices. In addition,

1 in 4 poll participants acknowledged sharing their work passwords with friends or acquaintances.

1.3 Evaluate the economic, operational, and societal effects of ransomware attacks on people and organizations.

Attacks using ransomware may have a negative financial, operational, or social impact on people or organisations. [4]

Impact on finances: Ransomware attacks frequently lead to financial losses due to ransomware payments, expenses related to data and system repair, and lost revenue during downtime.

Productivity and Operational Downtime: Organisations that encounter downtime due to system failure experience poorer productivity, slower business operations, and higher recovery costs.

Additional Security: In order to stop upcoming assaults, organisations frequently need to spend money on sophisticated cybersecurity measures, including threat detection software and employee training [7]. Costs are raised as a result of this. Publicly revealed ransomware attacks can harm people's and companies' reputations, confuse customers, and result in lost commercial possibilities and legal standing, with phishing scams playing a significant role [5,6].

Operational Activity:

Uptime and Service Outage: Ransomware assaults frequently compel businesses to shut down systems or services in order to stop the attack and re-establish functioning. The operations, vital business, customer service, and linked devices may all be significantly impacted by this outage.

Data Loss and Recovery: Occasionally, ransomware-caused data damage or encryption causes organisations to lose access to crucial data. Restoration operations are costly and time- consuming, necessitating either data recovery from backups or contracting with a cybersecurity firm.

Allocating employees and resources: Responding to a ransomware attack necessitates allocating resources, such as IT personnel and security experts, in order to continue working and take preventative steps while conducting an investigation. This might exhaust resources and have an impact on regular operations.

Impact on Critical Services: A ransomware assault on vital utilities, healthcare, or infrastructure might have a direct impact on people's lives [6]. It may disrupt life-saving utilities, including energy, transportation, and other necessities. Individual ransomware can result in the revealing of personal and sensitive information, such as financial information, passwords, or private information, which raises privacy and personal data problems.

This may result in financial fraud, identity theft, or other privacy violations that are harmful to one's religion and general well-being.

1.4 Find practical solutions to cybersecurity problems brought on by ransomware attacks.

Ransomware attacks have led to cybersecurity issues that need to be addressed using a thorough and multi-layered strategy [6,8].

Implement automatic, routine backups of crucial data to offline or cloud-based storage. Regular Data Recovery. This guarantees that data may be recovered even if systems are hacked without paying the ransom. To verify the reliability and accessibility of the backed-up data, test the restoration procedure frequently.

Strong Security Measures: Use current and effective antivirus and anti-malware programs on all systems and devices [2,7,8]. Implement network segmentation to prevent attacks from moving laterally via the network. Protect network traffic by using firewalls, intrusion detection and prevention systems, and secure web gateways.

To improve access control, enable multi-factor authentication (MFA) for user accounts. Maintaining the most recent security patches on all software, operating systems, and apps requires regular software updates. Ransomware may take advantage of flaws in obsolete software. When feasible, enable automatic updates to guarantee prompt patching.

Employee Education and Awareness: Instruct staff members about cybersecurity best practises, including how to recognize phishing emails, stay away from dubious downloads, and report any suspicious activity. To improve

awareness of and reaction to ransomware attacks, hold frequent training sessions and simulations. Establish clear guidelines for the management of

confidential information and the proper usage of corporate resources. Creating an extensive incident response plan that intimates the actions to be followed in the case of a ransomware attack is called incident response planning. Establish lines of communication and procedures to promptly alert required parties, such as IT teams, management, and law enforcement, as needed.

Risk Management for Third Parties and Vendors: Before entering into business relationships, verify the vendors' and third-party partners' security policies. Protect shared systems and data by requiring vendors to adhere to security standards, carry out regular security audits, and uphold robust security protocols.

Engage with experts in cybersecurity: Work with cybersecurity professionals to assess your company's vulnerabilities, offer advice on risk mitigation, and assist in the creation of individualised security solutions.

Security insurance: To lessen the financial impact of a ransomware attack, you might want to think about purchasing cyber insurance coverage. Examine the terms of the policy, the limits of coverage, and the specific requirements for making a claim.

1.5 Make suggestions for policymakers, businesses, and people on how to strengthen their cybersecurity posture and readiness.

Politicians, organisations, and people will need to embrace authentication solutions that repeal the shared secret paradigm and are easy for clients and staff to use if they are to overcome authentication difficulties [2,6,7]. They may most effectively ensure the security of important digital assets by following the eight guiding principles for authentication policies listed below:

Have a strategy that specifically deals with authentication - Although a good approach to authentication is only one part of an appropriate approach to cyber risk management, any cyber program that does not place a priority on strong authentication is sadly lacking in substance.

Recognize the security risks associated with shared secrets - Policymakers should promote the use of more secure alternatives like FIDO authentication standards. They make use of public key cryptography and keep keys on the user's device and never abandon it, in place of less secure first-generation MFA technologies like OTPs, which rely on shared secrets.

Make sure mobile authentication solutions are supported - As the use of mobile transactions rises, any policy that is not created to maximize the use of MFA in that environment would fall short of providing sufficient protection for transactions that are conducted there.

Don't suggest a single technology, instead, concentrate on standards and results - new and better technologies will keep appearing as the authentication sector experiences a time of rapid development. Governments should therefore concentrate on an authentication strategy that is founded on principles and permits the use of new technologies.

Select user-friendly authentication methods to encourage adoption - Users are frustrated by poor usability, which prevents widespread adoption. This "user friction" is dramatically

reduced by next-generation MFA solutions, which also provide even greater security benefits. Incentives to promote the use of next-generation multi-factor authentication (MFA) should be sought by policymakers to balance user experience and security.

Be aware that strong authentication is no longer hindered by the old restrictions, cost – One of the biggest barriers to the adoption of MFA was the fact that only a small number of enterprises could previously afford to use first-generation MFA systems. Numerous companies are now providing next-generation authentication systems that are easier to use, tougher than passwords, and less expensive to implement and operate.

Know how important privacy is - MFA solutions' privacy practices might differ widely; some of them watch users' every move or build brand-new databases of consumer data. These technologies create new, exposed caches of valuable information while raising privacy issues. Thankfully, many authentication firms today have embraced a "privacy by design" approach that reduces the amount of personal data retained on computers and maintains crucial biometrics on a user's device.

Use biometrics in the right way - The near-universal use of biometric sensors in mobile devices is creating new opportunities for safe identification while also simplifying the usage of technologies like face and fingerprint recognition. The ideal approach to employ biometrics in a multi-factor authentication system, however, is to match a biometric on a device to unlock a second factor. The concerns to privacy and security associated with systems that centrally store biometrics should be avoided by just storing and matching biometrics on a device.

II. EXISTING METHODS:

2.1 NetWalker Ransomware:

NetWalker, also known by aliases such as Malito, Koko, and KazKavKovKiz, is not a new threat, with its origins tracing back to August 2019. It was first identified in September 2019 and is employed by the cybercriminal group CIRCUS SPIDER as part of a ransomware-as-a- service model. The service operates as a restricted affiliate program, where affiliates are carefully vetted before being approved. While NetWalker mainly targets hospitals in the U.S. and Spain, it has a global reach and has been particularly active in the Asia-Pacific (APAC) region. Within the cybercrime world, it has earned a reputation as a "big game hunter."

This ransomware uses a tactic known as "double extortion," demanding payment from victims while threatening to release sensitive data [9], with ransom demands ranging between $1,000 and $3 million USD. It primarily exploited the COVID-19 pandemic to target healthcare organizations [10]. NetWalker relies on widely known tools, exploit kits, and living-off-the- land (LOTL) techniques, such as Mimikatz, PSTools, AnyDesk, TeamViewer, NLBrute, and others. It is developed using C++ and PLL programming languages.

The cybercriminals behind NetWalker are predominantly Russian-speaking, and they deliberately avoid infecting systems within Russia and the Commonwealth of Independent States (CIS). To encrypt victims' data, NetWalker uses a combination of the ChaCha encryption technique and Elliptic Curve Cryptography (ECC) [11]. Healthcare institutions are particularly vulnerable to ransomware attacks like this, which can result in the theft or exposure of sensitive information, including patient data, and cause significant operational disruptions.

NetWalker locks and encrypts victims' data using both ECC and ChaCha encryption. ChaCha is a fast and secure symmetric encryption algorithm that operates using a stream cipher model [12], encrypting data in a continuous flow of key-dependent random numbers, making it harder for attackers to predict or break the encryption.

In contrast, ECC is an asymmetric encryption method that relies on elliptic curve mathematics. Compared to traditional methods like RSA, ECC offers strong security with shorter key lengths. It is used for secure key exchanges and digital signatures, ensuring data encryption and verification of authenticity.

By combining ChaCha and ECC, NetWalker leverages the benefits of both algorithms. ChaCha provides efficient and strong encryption of data, while ECC enables secure key exchange and cryptographic operations. Together, these algorithms enhance the security of the encryption process, making it extremely difficult for unauthorized users to decrypt the data without the proper private key.

ChaCha Encryption Algorithm:

ChaCha is a symmetric encryption algorithm that operates with a 256-bit key. It is a variant of the Salsa20 algorithm. The ChaCha encryption process involves recursively using the same key and nonce (a random or unique number used once), which generates a keystream. This keystream is then applied to the input data in a bitwise manner to produce the encrypted message, or "ciphertext."

The inputs to ChaCha include:

- A 256-bit key
- A 32-bit counter, which can typically be set to zero or one. The counter is used to ensure each block of encryption is unique.
- A 96-bit nonce, sometimes referred to as an Initialization Vector (IV) in other encryption protocols.
- The plaintext, which can be of any length.
- The output is an encrypted message (ciphertext) of the same length as the input plaintext.

Pseudocode for ChaCha Algorithm:

```
chacha20_encrypt(key, counter, nonce, plaintext):
    encrypted_message = "" # Initialize the encrypted message
    for j = 0 upto floor(len(plaintext)/64) - 1:
        key_stream = chacha20_block(key, counter + j, nonce)
        block = plaintext[(j*64).(j*64 + 63)]
        encrypted_message += block ^ key_stream
```

```
if (len(plaintext) % 64) != 0:
    j = floor(len(plaintext)/64)
    key_stream = chacha20_block(key, counter + j, nonce)
    block = plaintext[(j*64)..len(plaintext)-1]
    encrypted_message += (block ^ key_stream)[0..len(plaintext) % 64]
return encrypted_message
```

Elliptic Curve Encryption:

An Elliptical Curve is an elliptical curve formed by the points that satisfy the following equation:

$y^2 = x^3 + ax + b$

with a separator at infinity, symbolized by the symbol "∞". Here, the coordinates are to be selected from a finite field of characteristics not greater than 2 or less than 3, otherwise the curve equation will be slightly more complex.

ECC encryption involves several mathematical operations:

1. Key Generation:
   - Select an elliptic curve and a base point G on the curve.
   - Choose a private key d, a randomly generated integer.
   - Compute the public key Q as Q = dG, where dG represents the scalar multiplication of the base point G by the private key d.
2. Encryption:
   - Convert the plaintext message M into a numeric representation.
   - Generate a random session key k.
   - Compute the elliptic curve point C as C = kG.
   - Encrypt the numeric message by adding the session key k to the numeric representation of the message modulo the order of the curve.
3. Decryption:
   - Compute the shared secret as S = dC.
   - Subtract the shared secret S from the encrypted message to recover the numeric representation of the plaintext message.

Elliptic Curve Diffusal Layer (ECDLP) complexity is the secret of ECC's power. The security of ECC greatly depends on the size of the finite field of the underlying elliptic curve and the length of the private key. By employing relatively modest key sizes, ECC can offer the same level of security as other methods that need considerably bigger keys.

2.2 WannaCry Ransomware:

WannaCry ransomware is the name given to a group of malicious software programs that encrypt files using a combination of RSA and AES encryption algorithms [13]. WannaCry gained widespread media attention in May 2017 when it infected thousands of computers around the world. WannaCry used a vulnerability called EternalBlue to target Microsoft Windows computers. The EternalBlue vulnerability was created by the NSA but was leaked to the public by a group of cybercriminals known as "The Shadow Brokers". WannaCry uses Windows Crypto API for RSA encryption as well as random key generation. The virus also contains a statically linked third-party AES implementation. This encryption method produced a unique encryption key for each compromised PC. The infection on the infected computer encrypted files, making it impossible for the user to read them. The assailants demanded Bitcoin ransom payments in exchange for the decryption keys needed to unlock the encrypted files.

WannaCry consisted of various components, the main two components were the worm component and the encryption component.

RSA Encryption:

Public-key encryption technology known as the RSA (Rivest-Shamir-Adleman) algorithm was developed by Ron Rivest, Adi Shamir, and Leonard Adleman [14]. It offers a safe way to exchange keys, encrypt and decrypt data, and perform digital signatures.

The modular arithmetic and mathematical features of huge prime numbers serve as the foundation for the RSA algorithm. Basic explanation of the RSA encryption procedure:

1. Key Generation:

To create an RSA key pair, we first select two prime numbers p and q. Then, we multiply p and q together to get the modulus N. The modulus is an important factor in the RSA algorithm. Next, we compute Euler's totient function, which is equal to (p-1)-q-1. This function helps us to figure out how many integers are equal to N.

Next, we choose an encryption exponent, which must satisfy the following conditions:

- It must be greater than 1
- It must be less than φ(N) and it must be coprime to φ(N)

Finally, we calculate the decryption exponent (d). The decryption exponent d is the modular multiplicative inverse of e modulo φ(N).

2. Encryption:

- Convert the plaintext message into a numerical representation (usually as a series of bytes).
- Break the message into blocks if necessary.
- For each block, the ciphertext is calculated as C = M^e (mod N), where M is the plaintext message represented as a number.

3. Decryption:

- For each ciphertext block C, the plain text message is calculated as M = C^d (mod N), where d is the decryption exponent.
- If necessary, convert the numerical representation of the decrypted message back into the original plaintext form.

RSA gains security by having difficulty in factoring huge composite numbers. It is computationally impossible to factor the modulus N into its prime factors, which is necessary to break RSA encryption, for sufficiently big prime integers.

Key sizes are frequently chosen to be big, frequently ranging from 2048 bits to 4096 bits, to strengthen the security of RSA and thwart attacks using contemporary computer capabilities.

PseudoCode for RSA Algorithm:

Select P, Q where P and Q are prime numbers, P ≠ Q Calculate n, where n = P * Q

```
Calculate Φ(n), where Φ(n) = (P-1)*(Q-1)
Select Random E such as: gcd (Φ(n), E) = 1, 1<E<Φ(n)
Calculate D, where d.e = 1 (mod Ψ(n))
Public key {E,n}
private key {D,n}
```

2.3 Locky Ransomware:

Locky ransomware first emerged in early 2016 and quickly became one of the most

widespread and dangerous ransomware outbreaks [15]. It is notorious for its advanced spreading techniques and ability to encrypt data on infected devices, making them unusable until the ransom is paid.

Locky is typically spread through malicious email attachments disguised as legitimate documents like Word or PDF files. These attachments are often part of phishing attacks, tricking users into opening them by posing as important files such as invoices or shipping notifications. Once the user opens the compromised attachment, the ransomware is activated, and the encryption process begins.

Locky encrypts data on the infected system using strong encryption algorithms like RSA and AES. This process happens quickly and affects various file types, including databases, photos, spreadsheets, documents, and videos. Encrypted files are given a unique extension to make them identifiable. Locky also encrypts data on network shares and removable media connected to the infected system.

After encryption, Locky typically displays a ransom note in a text file or as desktop wallpaper, informing the victim that their files have been encrypted. The note provides instructions for paying the ransom and obtaining the decryption key. Bitcoin is often requested for payment due to the anonymity it offers.

Locky is known to continuously evolve to stay ahead of security researchers. It uses obfuscated code, command and control infrastructure, and changes file extensions and names to evade detection. Some ransomware groups have also used Distributed Denial of Service (DDoS) attacks to pressure victims into paying, increasing the likelihood of receiving a ransom.

Locky's creators are highly organized and skilled, typically giving victims a limited time to pay, often within a week. Due to the strength of Locky's encryption, failing to pay usually results in permanent data loss. If the ransom isn't paid by the deadline, the attackers may delete files or raise the ransom amount to further pressure the victim into payment.

Locky uses both RSA and AES encryption methods to protect the victim's data. RSA is an asymmetric encryption method based on the difficulty of factoring large prime numbers. It uses a public key to encrypt data and a private key for decryption. Each infected computer generates a unique pair of RSA keys, with the attackers keeping the private key for decryption and using the public key to encrypt the victim's files.

AES, a widely used form of symmetric encryption, is both efficient and secure. It uses a private key to encrypt and decrypt fixed-size blocks of data. In Locky's system, a random RSA key is generated for each file, and this RSA key is used to encrypt the AES key generated by Locky. This combination of RSA and AES ensures both the security and authenticity of the victim's data.

The use of RSA for asymmetric encryption and AES for symmetric encryption allows Locky to benefit from both technologies. RSA handles the exchange of keys, while AES encrypts the file contents directly. Without access to the attackers' private key, it is almost impossible for unauthorized parties to decrypt the data. This combination creates a secure and reliable encryption system.

In a Locky attack, the victim's data is encrypted with AES, while the AES keys are encrypted with RSA. This method effectively locks the data, making it nearly impossible to recover without the attacker's private key.

By October 2020, security experts noticed that some ransomware groups had started using DDoS attacks on victims' networks or websites to further pressure them into paying the ransom. At that time, only SunCrypt and RagnarLocker were using this tactic.

The current threat landscape has evolved, giving ransomware groups new opportunities to attack and pressure businesses into paying ransoms. Healthcare organizations are especially vulnerable, as attackers target them for quick and substantial profits.

2.4 Scareware:

Scareware is a type of malicious software that manipulates users through deception and fear, making them believe that their computer is infected with malware or facing other security threats [16]. Sometimes referred to as rogueware or fake antivirus software, scareware relies heavily on social engineering techniques to trick users into taking undesirable actions, such as purchasing bogus security software or disclosing personal information.

This software often generates fake security warnings, pop-ups, and system alerts designed to create a sense of urgency and panic. It frequently poses as legitimate antivirus tools or system optimization software, making it challenging to identify. Scareware is typically distributed via spam emails, malicious websites, compromised advertisements, or through software bundles containing other programs.

One common method of attack is the drive-by download, where users unknowingly download malware by visiting fraudulent websites [17]. Additionally, scareware may present users with fake system scans and exaggerated virus detection alerts, pressuring them into taking immediate action. It can also hijack a user's web browser, redirecting them to malicious sites or blocking legitimate access.

Scareware's main strategy involves providing fake scan results, falsely claiming the presence of viruses or overstating the severity of harmless files [18]. This manipulation drives users to purchase fake software as the only apparent solution. Furthermore, scareware can trick users into making fraudulent payments, stealing sensitive information like credit card details by using insecure networks.

The consequences of falling victim to scareware can be significant. Users may suffer financial losses by purchasing fraudulent software or services. If personal information is submitted, identity theft becomes a risk, and certain scareware variants may even introduce additional malware or vulnerabilities to the victim's system, compromising security further.

Unlike ransomware, which employs advanced encryption techniques to lock a victim's data, scareware does not typically encrypt files. Instead, it depends on psychological manipulation, using pop-ups and fake user interfaces to deceive the victim. The main objective of scareware is to create fear and induce users into purchasing false software or disclosing personal data, rather than locking files or preventing access.

While scareware generally avoids encryption, it could potentially utilize encryption algorithms similar to those employed in ransomware. These might include symmetric encryption methods like AES or 3DES, which use a single key for both encryption and decryption. Alternatively, scareware could adopt asymmetric encryption methods such as RSA or Elliptic Curve Cryptography (ECC), where a public key is used to encrypt data, and a private key is needed to decrypt it.

In a hypothetical scenario, scareware might use a hybrid encryption approach, employing symmetric encryption for efficiency and then encrypting the symmetric key with asymmetric encryption to ensure secure key exchange. However, it is essential to note that scareware's primary focus is on deception rather than encryption. If encryption techniques are used, it is often to create the illusion of legitimacy. The core strategy of scareware remains focused on social engineering and fraudulent user interfaces, rather than complex cryptographic methods.

To protect against scareware, users should use trusted antivirus software, ensure their systems and applications are updated, and exercise caution when confronted with sudden pop-ups or alarming alerts. Awareness and education about scareware's deceptive tactics can further help users avoid falling victim to such scams.

2.5 Emotet:

Advanced Trojan Emotet is often disseminated by phishing email attachments and URLs [19] that, when opened, activate the payload, using shared devices to write to and brute-forcing user credentials, the virus then makes an attempt to spread throughout a network.

Emotet is hard to get rid of because of its "worm-like" traits that take into account network- wide infections. Additionally, Emotet regularly updates and expands its capabilities by using modular Dynamic Link Libraries [20].

Indicators for emotets have suggested a rise in activity beginning in 2020. The federal, civilian executive branch networks are protected by CISA's EINSTEIN Intrusion Detection System, which has discovered around 16,000 alerts related to Emotet activity. According to CISA, Emotet was being utilized gradually throughout ostensibly targeted activities. Emotet used hijacked Word documents (.doc) contained in phishing emails as its first insertion vectors.

2.6 CryptoLocker Ransomware:

Some ransomware just locks your machine and demands payment [21]. With CryptoLocker, however, your personal information, including documents, spreadsheets, and photos, are encrypted while your computer and applications continue to function normally.

The sole copy of the decryption key is kept by the thieves on their server; it is not saved on your computer, making it impossible for you to open your data without their help. After that, they provide you a little window of time (such as three days or 72 hours) to pay for the key.

Since the decryption key is exclusive to your computer, you cannot just use another person's key to decode your data.

Bitcoin's pseudonymous and decentralized nature makes it ideal for ransomware operations, providing attackers with substantial anonymity during ransom transactions [22].

How CryptoLocker works:

1. CryptoLocker installs itself into your Documents and Settings folder and adds itself to the registry list of programs that Windows automatically runs when you log in, using a name that is chosen at random.
2. Under the domain extensions.biz,.co.uk,.com,.info,.net,.org, and.ru, it generates a lengthy list of what seem to be arbitrary server names.
3. It tries to create a web connection with each of these server names in turn until it finds one that responds.
4. The program uploads a little file that serves as your "CryptoLocker ID" after finding a server it can connect to. CryptoLocker's infiltration methods typically involve phishing schemes that lure victims into downloading malicious attachments, thus allowing the ransomware to begin its infection sequence on the user's machine [23].
5. Your computer is then sent the public key section. The server then generates a pair of public and private keys unique to your ID.
6. The virus on your computer encrypts any files it can find that match a long list of extensions, such as spreadsheets, pictures, and documents, using this public key.
7. After that, the virus displays a "pay page," providing you a little window of time, usually 72 hours, to pay a fee, usually $300, to get the secret key to your data returned. Surprisingly, the price point is still the same as it was in 1989.

Based on the type of key used, there are two different types of cryptographic algorithms:

1 Symmetric
2 Asymmetric

Before going into the algorithm, let's make a few assumptions: the sender is the one who encrypts the data before sending it, and the receiver is the one who uses a key to decrypt it.

1 Symmetric key [24]

In symmetric key encryption, both the sender and the receiver use the secret key, also referred to as the sender key. Data is encrypted by the transmitter and decrypted by the receiver using the same key.

A symmetric key is utilised by the following algorithms:

- RC4
- AES
- DES
- 3DES
- BlowFish

2 Asymmetric key [25]

Symmetric keys are simpler to use, but the difficulty of safely exchanging keys still exists. Key exchange has been made possible by a public or asymmetric key, a set of two keys that are both public and private. In contrast to a public key, which may be shared in an insecure manner, a private key is always retained by the owner in confidence. The other key can be used to decrypt with either key, and vice versa. The most popular algorithms are:

- RSA
- Diffie Hellman
- ECC
- DSA

III. RESULTS:

Through the COVID pandemic, we came to see how vulnerable our network security really is. According to reports 20% of companies experienced security breach in their security during the pandemic [1]. We like in such an era in which cyber-attacks happen every second and millions of dollars are lost as ransom. More than two thousand attacks happen all across the globe. Also, the pandemic helped in these cybercrimes to increase and the number of attacks reached an all-time high during the COVID.

In order to understand cyberthreats and cyberattacks during the epidemic, we examined a number of reports and journals. According to those statistics, phishing and social engineering attacks [6] were the most often used types of attacks by hackers and cybercriminals to break security. According to studies, 35% of all social engineering techniques involved phishing. Spam is the second most used social engineering attacks, with a usage rate of 16%. Scams were the third most popular tactic, used 14% of the time. Scams generally occurred through SMS, OTP and fraud emails.

Numerous inventive techniques have been created to protect networks from various DDoS attacks [8]. Several machine learning techniques have been developed to identify DDoS attacks in cloud computing [8]. ELMs are classified as Single Hidden Layer Feed-Forward neural network structures (SLFN) [26], a subset of Artificial Neural Networks (ANNs). This model's main selling feature is that the hidden biases and connection weights between the input and hidden layers are both initialised with random values. The weights between the hidden and output layers are chosen using the Moore-Penrose inverse technique.

A few of the evolutionary optimisation techniques that are available for improving ELM parameters are competitive swarm optimisation, particle swarm optimisation, and differential evolution, these methods are enhanced by combining swarm-based exploration capabilities to find optimal solutions in high-dimensional spaces [27]. The self-adaptable evolutionary extreme learning machine (SaE-ELM), which incorporates novel qualities [28] to quickly determine the optimal values for ELM parameters, is introduced in this study. During the evolution process, SaE-ELM may automatically choose the most effective mutation method and update the crossover rate. However, it only employs one crossover operator at the moment.

In IoT and social networking sites within cyber security applications, we got to understand that intelligent algorithms play a critical role [7] in improving performance metrics like threat detection which helps to detect threats, throughput of the network, end-to-end delay, packet delivery, and detection of different vulnerability.

Techniques for machine learning include reinforced adaptation, unsupervised adaptation, and supervised adaptation. For tasks like data categorization, outlier identification, dimensionality reduction, feature subset extraction, and transformation, these techniques are used within the learning model. machine learning methods like unsupervised learning are essential in detecting outliers and enhancing feature selection for robust anomaly detection [29].

For particular cyber security issues, machine learning algorithms perform better when based on paradigms inspired by nature. To increase the effectiveness and precision of the learning model, NIC algorithms optimise weight values, parameter tuning, feature subset extraction, and feature selection. NIC algorithms, inspired by evolutionary and nature-based strategies, offer effective solutions for optimizing feature selection and tuning in cybersecurity applications [30].

Deep learning algorithms outperform conventional shallow learning architectures because they use numerous hidden layers with unique hidden nodes. In terms of throughput, packet delivery, end-to-end delay, energy consumption, and learning performance, they demonstrate higher learning abilities, which leads to positive results. Large datasets, GPU system acceleration, and the use of intricate activation functions make deep learning models particularly suited for these tasks. deep learning approaches in cybersecurity are optimized for low energy consumption, allowing for resource-efficient and scalable applications in IoT and constrained networks [31]

IV. DISCUSSION:

Millions of people's daily lives as well as technology and cybersecurity were significantly impacted by the COVID-19 epidemic. The world's population had become accustomed to remote jobs, online education, and an increasing reliance on digital platforms, making the flaws and dangers of cyberspace more apparent than ever. Cybercriminals swiftly exploited the uncertainty and confusion, launching highly successful attacks to profit from the circumstance [1].

Businesses across all sectors faced an extraordinary spike in cyber dangers as millions of workers began working remotely. Cybercriminals targeted the growing use of cloud services, collaboration tools, and video conferencing platforms as well as the vulnerabilities of hastily implemented remote access solutions. Hackers increased their phishing attacks, ransomware incidents, and data breaches by preying on people's worries and confusion about the epidemic [3]. These threats have not only resulted in monetary losses but have also jeopardised the security of critical systems, compromised personal information, and disrupted essential services.

In this review paper we explored the different types of cyber-attacks used during the pandemic and also looked at some new machine learning algorithms which have been developed to prevent attacks like DDoS, and spoofing. Intelligent algorithms are helping to prevent intrusion attacks and can also detect malware in MANETs.

Numerous studies have found a marked increase in scams and malware attacks since the pandemic's beginning. Phishing attacks specifically soared by 600% in March 2020 [5]. According to the World Economic Forum (WEF), there were 30,000 COVID-19-related cyberattacks between December 2019 and April 2020 [2], a 50.1% increase from the previous year. CGI discovered an astonishing 30,000% increase in cyberthreats for COVID-19. Interpol detected a large number of spam emails, malware instances, and dangerous URLs linked to COVID-19 during the first four months of 2020. Ransomware payouts also saw a significant increase, with an average payment of $178,254 in the second quarter of 2020. In April 2020, Google reported that every day, 18 million emails containing malware and phishing were blocked.

The impact of these cybercrimes was greater on the organisational level. Ransomware was a tool that was widely utilised and had an effect on healthcare services [4]. Numerous nations, including the United States, France, Spain, the Czech Republic, and others, have reported ransomware attacks. Health organisations were targeted by ransomware like NetWalker, and since thieves knew that these organisations were likely to pay ransoms to prevent the loss of patient lives, significant losses were reported.

More notable instances of malware during the pandemic include the following: Malware is routinely downloaded and installed on victims' devices using a trojan named Trickbot. According to Microsoft, Trickbot is the malware operation that uses COVID-19-related attack techniques the most frequently [6]. An MBR rewriter is a different class of malware that wipes out the MBR on a device's CDs, rendering them worthless. The app Corona Live 1.1 also gained access to the device's camera, location data, photographs, and videos by using a valid COVID-19 tracker that was made public by John Hopkins University.

V. CONCLUSION:

The pandemic exposed the security flaws which were prevalent in our systems. Due to the pandemic, new techniques and machine learning algorithms came up in order to detect and prevent network disruption.

Although our existing security measures were able to prevent a lot of security attacks, it is extremely important to follow strong protocols and keep personal data securely. There are many ways in which a person can reinforce his or her security and prevent frauds and cyber-attacks. The most important tip is to always use a strong and unique password for every application you use. Keeping the same password for multiple accounts can mean that if the attacker cracks one of the passwords, he automatically gets access to all other accounts.

It is a good practice to enable two factor authentication on different apps. Two factor authentication helps to prevent hackers from getting unauthorised access. Generally, users use Single Factor Authentication or password-based authentication in which a user creates a unique password and then uses it to access data, better security can be established by using two factor authentication which adds one more layer of security by reverifying if the user is actually the person he claims to be. Two factor Authentication uses different methods like OTP, SMS and fingerprint to reverify the user's authenticity.

Cybercrimes have dramatically expanded as a result of the epidemic, posing major risks to people, businesses, and even governments. Fraudsters today have an easier time identifying flaws and executing sophisticated attacks due to the increasing reliance on digital platforms and technologies. The range and level of sophistication of cybercrimes have reached previously unheard-of heights during current global crisis. These offences range from ransomware attacks and phishing scams to identity theft and online fraud.

In this review paper we have also explored the different ransomwares which were used during the pandemic and also some machine learning algorithms and intelligent algorithms which have been developed to reduce cybercrimes.Finally, it is essential to recognize that while we navigate the evolving environment of the digital world, it is critical for individuals and organisations to keep alert, adopt robust security measures, and collaborate with law enforcement officials and cybersecurity experts.

REFERENCES

[1] P. G. Altbach, Monica T Whitty, Nour Moustafa, Marthie Grobler, Cybersecurity when working from home during COVID-19: considering the human factors, Journal of Cybersecurity, Volume 10, Issue 1, 2024, tyae001, https://doi.org/10.1093/cybsec/tyae001

[2] OECD (2020), "Seven lessons learned about digital security during the COVID-19 crisis", OECD Policy Responses to Coronavirus (COVID-19), OECD Publishing, Paris, https://doi.org/10.1787/e55a6b9a-en.

[3] Pranggono, B., & Arabo, A. (2020), COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), e247, https://doi.org/10.1002/itl2.247

[4] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University. Computer and information sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

[5] Abroshan, Hossein & Devos, Jan & Poels, Geert & Laermans, Eric. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3109091.

[6] Hijji, Mohammad & Alam, Gulzar. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/ Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3048839.

[7] Subashini, Parthasarathy & Krishnaveni, M & Dhivyaprabha, Tt & Shanmugavalli, R. (2020). Review on Intelligent Algorithms for Cyber Security. 10.4018/978-1-5225- 9611-0.ch001.

[8] Kushwah G. S. and Ranga V., Optimized extreme learning machine for detecting DDoS attacks in cloud computing, Computers and Security. (2021) 105, 102260, https://doi.org/10.1016/j.cose.2021.102260.

[9] Al-rimy, Bander & Maarof, Mohd & Shaid, Syed. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security. 74. 10.1016/j.cose.2018.01.001.

[10] Anagnostopoulos, Marios & Kambourakis, Georgios & Kopanos, Panagiotis & Louloudakis, Georgios & Gritzalis, Stefanos. (2013). DNS Amplification Attack Revisited. Computers & Security. 39. 10.1016/j.cose.2013.10.001.

[11] Hankerson, Darrel & Menezes, Alfred & Springer, Scott. (2004). Guide to Elliptic Curve Cryptography. 332. 10.1007/978-1-4419-5906-5_245.

[12] Sabyasachi Dey, Tapabrata Roy, Santanu Sarkar. Revisiting design principles of Salsa and ChaCha. Advances in Mathematics of Communications, 2019, 13(4): 689-704. doi: 10.3934/amc.2019041

[13] Mohurle, Savita & Patil, Manisha. (2022). A brief study of Wannacry Threat: Ransomware Attack 2017. INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY. 8.

[14] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120–126. https://doi.org/10.1145/359340.359342

[15] Scaife, Nolen & Carter, Henry & Traynor, Patrick & Butler, Kevin. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. 303-312. 10.1109/ICDCS.2016.46.

[16] Garfinkel, Simson & Shelat, Abhi. (2003). Remembrance of data passed: A study of disk sanitization practices. Security & Privacy, IEEE. 1. 17 - 27. 10.1109/MSECP.2003.1176992.

[17] Jakobsson, Markus. (2016). Understanding Social Engineering Based Scams. 10.1007/978-1-4939-6457-4.

[18] Jakobsson, Markus & Ratkiewicz, Jacob. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features.. 513-522. 10.1145/1135777.1135853.

[19] Kuraku, Sivaraju & Kalla, Dinesh. (2020). Emotet Malware -A Banking Credentials Stealer. 10.9790/0661-2204023140.

[20] Suthar, F., Patel, N., & Khanna, S. (2022). A signature-based botnet (emotet) detection mechanism. Int. J. Eng. Trends Technol, 70(5), 185-193.

[21] K. Liao, Z. Zhao, A. Doupe and G. -J. Ahn, "Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin," 2016 APWG Symposium on Electronic Crime Research (eCrime), Toronto, ON, Canada, 2016, pp. 1-13, doi: 10.1109/ECRIME.2016.7487938.

[22] Masarah Paquet-Clouston, Bernhard Haslhofer, Benoît Dupont, Ransomware payments in the Bitcoin ecosystem, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz003, https://doi.org/10.1093/cybsec/tyz003

[23] Evin, Thenuka. (2021). Analysis on the crypto locker ransomware.

[24] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[25] Silva, C., Cunha, V.A., Barraca, J.P. et al. Analysis of the Cryptographic Algorithms in IoT Communications. Inf Syst Front 26, 1243–1260 (2024). https://doi.org/10.1007/s10796-023-10383-9

[26] Bacanin, N., Stoean, C., Zivkovic, M., Jovanovic, D., Antonijevic, M., & Mladenovic, D. (2022). Multi-Swarm Algorithm for Extreme Learning Machine Optimization. Sensors (Basel, Switzerland), 22(11), 4204. https://doi.org/10.3390/s22114204

[27] Rick Boks, Hao Wang, and Thomas Bäck. 2020. A modular hybridization of particle swarm optimization and differential evolution. In Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion (GECCO '20). Association for Computing Machinery, New York, NY, USA, 1418–1425. https://doi.org/10.1145/3377929.3398123

[28] Cao, J., Lin, Z., & Huang, G. (2012). Self-Adaptive Evolutionary Extreme Learning Machine. Neural Processing Letters, 36(3), 285-305.

[29] Heigl M, Weigelt E, Fiala D, Schramm M. Unsupervised Feature Selection for Outlier Detection on Streaming Data to Enhance Network Security. Applied Sciences. 2021; 11(24):12073. https://doi.org/10.3390/app112412073

[30] Hiremath S, Shetty E, Prakash AJ, Sahoo SP, Patro KK, Rajesh KNVPS, Pławiak P. A New Approach to Data Analysis Using Machine Learning for Cybersecurity. Big Data and Cognitive Computing. 2023; 7(4):176. https://doi.org/10.3390/bdcc 7040176

[31] Shukla, Surendra & Pant, Bhasker & Bordoloi, Dibyahash. (2021). DEEP LEARNING AND DATA MINING APPLICATIONS IN THE CYBERSECURITY PARADIGM TO FIGHT CYBER-ATTACKS. 18. 1735-188. 10.29121/ WEB/V18I4/128.