Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 3 March 2023

Research Article

Encryption: A Threat to Cyber Attack

Anushka Sharma*

School of Electrical and Electronics Engineering, Vellore Institute of Technology Chennai, Tamilnadu, India

***Corresponding Author:** Anushka Sharma, School of Electrical and Electronics Engineering, Vellore Institute of Technology Chennai, Tamilnadu, India.

Received: January 11, 2023

Published: February 02, 2023

Abstract

Data security and privacy are the most critical parts of any organization. In this digitalization era, we live in a world where data is maintained through various software without human intervention. Social networking sites are a fundamental part of our day-to-day life, where people can not only have conversations. Still, they can share their data without hesitation, but they are unaware that cyber-criminals can continue to focus on these social platforms to steal all sorts of personal data. Not only in social media but bank transactions too, which are taking place online nowadays, an individual must ensure all kinds of security measures to keep hackers away from crucial data. Encryption is a method of transforming all sorts of data into secret code which no one, including eavesdroppers or hackers, can easily scan. In this method, all kinds of messages, data, and information can be turned into cipher text which, with the help of a shared key, is scanned or specified; however, the message has to be encoded for this method to get implemented. With the help of the encryption method, we can use specific hidden secret codes that can only be accessed by the authorized user and will remain out of reach for the hackers. Even if the hacker succeeds in cracking the password still, accessing the target data will be much more difficult as he will be required to crack several codes necessary for accessing different folders before reaching the target folder (misleading the hacker from the target file) and to make the things worse for the hacker/attacker, a time limit is applied on the target folder after which the attacker can be thrown out of the system. The system itself can identify the attacker from the authorized user.

Once the attacker is thrown out of the system, the password gets changed automatically so the hacker can no longer enter the system using the hacked password.

Keywords: Digitalization; Cipher; Cyber-criminals; Encryption; Secret Code

Introduction

When you hear the word "hacker", what is the first thing that comes to your mind? Most people think some a mysterious person wearing a hoodie with black nail polish, a laptop or a computer with snarky stickers and a string of empty energy drink bottles or cans encompassing them. Generally, these hackers plan an attack strategy in a sophisticated manner so that people will never know that they are becoming a victim of tons of common attacks even while managing their online accounts with security measures. So, if you are trying to find a solution to be safe, the first and foremost thing is to have a secure password to enhance cybersecurity and save the data from attackers.

Everyone has a minimum of once in their period set a word with their birth date and year. Folks typically prefer exploiting their personal information as a password so it'd be easier to remember. However, such unsafe and insecure passwords are simply hacked and broken into by totally different hackers worldwide. Hackers devise a typical pattern to be quickly ready to crack our password and hack into our system. Word attacks merely ask for our pass-

word to be taken by a hacker. In step with analysis in 2020, 81% of knowledge breaches were caused thanks to be unsecured and compromised credentials.

Due to digitalization, access to almost everything is possible, including the personal data of each and everyone present on the internet; hence with these advancements, the significance of cybersecurity [1-3] is playing its essential role in protecting one's data, network, programs and other information against any kind of attack taking place in today's world. For methods implemented under cyber security to work well, one needs to keep two essential elements during securing data, i.e. data at rest and data in transit, effective monitoring and logging of data access [4]. Not only is cyber attack harmful to those who use online transactions, but even the students in school are not safe due to their data being saved in various software and, once hacked, can become a threat to their lives too!!!! Hence, it is recommended to keep updating the passwords and all related security measures once a month or two to avoid such threats to privacy.

Literature Review

The focus of the work in this regard is on examining possible ways to prevent password attacks and the tools and techniques available that are used to avoid such attacks. Several researchers examined cybersecurity. In "Prevention of the Persistent Cross-Site Scripting Attack by applying a pattern filtering approach" by I. Yusof, the XSS attack was prevented by using the pattern filtering method in which user input was sanitized before saving data in the database. A web browser takes user input as untrustworthy data, which goes through the filtering process to obtain a "clean" status. This clean data is stored in the database to generate a clean output from this output cleanup. In "Defending against web vulnerabilities and Cross Site Scripting" by T. Venkat Narayana Rao, the XSS vulnerabilities are with the -Defense coding removed practice that validates and sanitizes inputs. Notes are used in "Notes: A Client-Side Solution to Mitigate Cross-Site Scripting Attack" by E. Kirda. The first client-side solution mitigates cross-site scripting attacks and automatically generates rules to prevent cross-site scripting attempts. Notes efficiently protect against the loss of information from the user's environment. It requires minimal user interaction and effort in "Defeating Script Injection Attacks with Built-in Browser Policies "by T. Jim and N. Swamy to prevent XSS by using built-in policies enforced by the browser [5-7].

Methods

Passwords are one of the most common verification tools of an option for many people, so attacking those passwords of individuals more often becomes an attraction for hackers. Implementing a few different methods can be done appropriately. Often, people forget their passwords, so to avoid this, they keep some copies of their passwords in notes around their working desks. This becomes so vulnerable that anyone can search and find the password and, with the intention of harm, can attack an individual. Also, attackers may attempt to interfere in the network transmission process, which is not secured or encrypted by the network. Through social engineering, they can easily manipulate their targets to input their password to resolve any critical problem.

In some cases, the attacker can guess the user's password, especially those with no upper case or special characters and just the "abcdef" thing. Attackers also use brute-force methods to guess the passwords, which uses the primary data related to the person or their job to guess their password [8,9]. For example, their birthdate, date of anniversary, nicknames or other people; however, easy-to-discover details are often employed in different mixtures to decipher their password. People's data on social media can also become vulnerable towards brute-force password hacking. A person who will come just for fun can keep especially the names of their pets, kids or hobbies as their password, which becomes an easy task for the brute-force attacker to guess. Hackers can also use dictionary attacks to obtain user passwords. A dictionary attack is a technique that uses common words and phrases, for example: Trying to guess the word of the target password from the dictionary. Configuring blocking policies is an effective way to prevent brute force attacks and dictionary passwords. After a certain number of unsuccessful attempts, this will automatically block access to the device, website or application. With the blocking strategy, the attacker has only a few attempts before being denied access. If we already have a lockout policy and find that our account has been locked due to too many login attempts, we recommend that you change your password. If attackers continue to use brute force or dictionary attacks to guess the password, they may write down passwords that do not work. For example, if our password is our last name, then our year of birth, and the hacker tried to put our year of birth before our previous name the last time they tried, they may be correctly identified the next time they try. Now let's see some types of passes. Phishing is when an attacker acts like a person from a trusted

source sends a person a fraudulent e-mail, which in turn asks to share some personal data in the form of resetting the password; sometimes, these links can install malicious software on the device. A man-in-the-middle- this attack (MitM) occurs when a hacker or an infected system stands uncompromisingly between two people or systems and decrypts the information (including passwords) transmitted to each other.

- **Brute force attack:** If the password to open the door with the key matches, a brute force attack is used. A hacker can verify 2.18 trillion password and username combinations in 22 seconds. If our password is simple, our account may be stolen.
- **Dictionary attack:** It is a brute force based choosing "basic" words for passwords, the most common of which is compiled by hackers in "crack dictionary", More sophisticated dictionary attacks use words that are personally important to one, such as baby's name or pet's name
- **Credential stuffing:** If we have been attacked, we will know that our old password may have appeared on a suspicious page. Fill in the credentials to use an account whose password has never been changed since the account was hacked. Hackers will try different username and password combinations, hoping the victim will never change them.
- **Keyloggers:** It is malware designed to track every keystroke and reports the hacker usually. User download software that is considered legitimate only to install the keylogger without notice.

Preferred solutions to prevent cyber attacks

We can protect the data from phishing attacks by doing the following:

- **Check the e-mail to know about the sender:** Check the "From:" line in each e-mail to get confidence that the person specified matches the expected e-mail address.
- **Check the source:** If in doubt, try contacting the person who sent the e-mail to ensure he is the sender.
- **Please consult our IT department:** Your company's IT department will usually tell you if the e-mail you receive is legitimate.

How to prevent multiple man-in-the-middle attacks

- **Enable encryption on our router:** If someone on the street has access to our modem and router, they can use sniffer technology to see what information they are transmitting.
- **Use robust data to fill and two-factor authentication:** Once set, many router credentials, passwords and usernames do not change from time to time. Hackers can redirect all our traffic to their infected server if they control our router.
- **Use VPN:** A secure virtual private network (VPN) can ensure that all servers you send data are reliable, which helps prevent many man-in-the-middle attacks.

Prevent brute force attacks

- **Use strong passwords:** The difference between a lowercase six-digit password and a password that mixes characters and numbers is enormous. As our password becomes more complex, the chances of brute force attacks become less.
- **Enable and configure remote access:** Always ensure ourselves from the IT department if the company uses remote access management. By using the control tools like OneLogin, one can quickly reduce the threat of brute force attacks.
- **Multi-factor authentication is required:** After enabling Multi-Factor Authentication (MFA) for our account, potential hackers can only send a request to the second factor to access our account. Hackers will most likely not be able to access our mobile device or fingerprint, which means they will not be able to access our account.

Prevent dictionary attacks

- **Never use words in the dictionary as passwords:** If you have read it in a book, it should never be part of our password. Consider using a password management system if you need to use passwords instead of access control tools.
- **The account was locked after too many password errors:** It can be frustrating to lock our account if you temporarily forget our password, but the alternative is usually an insecure account. Try five times or less before the app prompts you to calm down.

- **Consider using a password manager:** The password manager will automatically generate complex passwords to prevent dictionary attacks.

Prevent fraudulent login information

- **Manage our account**: Services like haveIbeenpwned.com to check if our e-mail address is related to a recent leak.
- **Change the password regularly**: The longer the password remains the same, the more likely a hacker will find a way to crack it.
- **Use a password manager:** Like dictionary attacks, strong and secure passwords can prevent many credentials-stuffing attacks. The password manager helps with maintenance.

Protect ourselves from keyloggers

- **Check our physical hardware:** If someone has access to our workstation, you can install a hardware keylogger to collect information about our keystrokes. Check our computer and surrounding area regularly to ensure you are familiar with each device.
- **Perform a virus scan:** Use reliable antivirus software to scan our computer regularly. Antivirus companies keep logs of the most widespread malware keyloggers and mark them as dangerous.

A longer password is required. It turns out that longer passwords and passphrases can significantly improve security [10-12]. However, it is still crucial to keep in mind that applying longer passwords which may have been guessed previously, can also make the data and personal details vulnerable to several cyber-attacks.

- **Do not use any personally identifiable information:** By taking the consent of the user's details, these kinds of passwords encourage them to create a particular password. As mentioned above, most users use personal information to create passwords, such as hobbies, nicknames, pets, or family members' names. If the hacker can access the personal data of a particular user (for example, via social networks), use this information to check the password combination. At the very least, passwords should be checked to ensure they do not contain essential information. B. User name or credentials.
- **Use different passwords for different accounts:** Password policies should require users to distinguish between security and convenience and prevent users from using the same password for all their accounts. Use the same computer-you must use a different password.
- **Accept standard passwords:** Some password policies require users to create passwords instead of passwords. Although passphrases have the same purpose, they are often more difficult to crack due to their length. A valid password should contain numbers and symbols as well as letters. It is easier for users to remember passwords than to remember passwords.
- **Discourage sharing:** The password policy should stipulate that the password should be private and cannot be transmitted between users. Use the two-way authentication process. The proof before login is usually by sending the password and temporary code to a mobile phone, e-mail or other means.

Even after precautions, if a hacker attacks the system containing many confidential data, how can it be protected?

To protect such data from hackers on a large scale, we can use encryption methods to secure the data under IoT systems against cyber-attacks. Some new solutions and ideas which can help prevent a cyber-attack are illustrated below;

- Use of multi passwords in a layered manner or differently applied encryption for authorized and unauthorized access.
- Even if the attacker cracks the passwords and enters into the system still then he can't directly access the folder containing confidential data as the access to the target folder will be through several folders; for example, if data is stored in folder 9, then first, he will have to go to folder 1 from which he will be directed towards folder 2 then folder 3 and so on, this will become a very tedious task for him to find the data going through a large number of folders.
- Whereas the genuine person with the authority of access will go directly to the targeted folder by inserting a secret code and accessing the data directly.

- Now the attacker, unaware of the secret code while navigating through the layer of folders, will have time limitations to open every folder, failing which he will be thrown out of the system. And even if he succeeded in reaching the targeted folder, there will also be minimal time for the attacker to avail as the system distinguishes the attackers coming through the layer of folders.
- Once the attacker is thrown out of the system, now automatically, the password will get changed to another one which the authorized person had set.
- In his first access, the genuine user will be allowed to set at least 4 passwords which can be used sequentially whenever the system identifies any attack. A simple demo is given below, showing what can happen when a user and an attacker enter the system.

Figure 1, given below, shows how the attacker enters the system and what can happen to him.

Figure 1: Attacker entering the system

We will be using AES encryption using python programming. The options of AES are as follows –

- Bilateral key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Give full specification and style details
- Computer code which can be implemented using languages like java and C
- AES rule enclosed the following:
- Security-Keeping in mind the competition, the strength of security was to be thought of as one of the necessary things. Compared to alternative submitted cyphers, competitive algorithms were judged based on their ability to resist attack.
- Cost-Most of the candidate algorithms were judged based on the procedure and memory efficiency. The cost is meant to be discharged on a global, nonexclusive, and royalty-free.
- Implementation. Factors to be considered include the algorithm's flexibility, hardware or computer code implementation quality, and overall simplicity.

AES is a repetitious instead of a Feistel cipher. It's supported 'substitution–permutation network'. It includes a series of joined operations that involve replacement inputs by specific outputs (substitutions) involving shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These 16 bytes are organized in four columns and four rows for the process as a matrix – in contrast to DES, the amount of rounds in AES is variable and depends on the length of the key [13-16]. AES uses ten spherical for twelve 8-bit keys in figure 2, 12 rounds for 192-bit keys and fourteen rounds for 256-bit keys. Each round uses a unique 128-bit round key calculated from the first AES key.

Figure 2: Schematic of AES structure.

AES is one of the encryption methods where we tend to prohibit the description of a typical spherical AES encryption. Every round comprises four sub-processes figure 3. The primary round process is portrayed below.

Byte substitution

This substitution consists of 16 input bytes by making an S-box; the result is indicated by a matrix of 4 columns and rows. Every four rows are shifted to the left by using shift rows in the matrix. Any kind of mentions indicated as 'fall off' are inserted again on

Figure 3: Primary round process of AES structure.

the proper arrangement of the row. A shift is used when – if the first row doesn't get shifted, the second and third row gets shifted to one position and 3 bytes, respectively; in addition to this, the 4th row to is shifted three positions to left, which results in a replacement of matrix which contains 16 input bytes.

Mix columns

Every column consisting of four bytes in this arrangement gets some mathematical work to operate. This performs the replacement of the 1st column by taking the input of 4 bytes of one column and, as an output, provides four new bytes, which further results in the generation of 16 new bytes.

Addroundkey

The 16 bytes of the matrix are now thought-about as 128 bits and are XORed to the 128 bits of the round key. If this can be the last round, then the output is the ciphertext. Otherwise, the ensuing 128 bits are taken as sixteen bytes, and we begin associate other similar spherical.

The method of coding [16-19] - a comparison takes place between the decryption process of an AES ciphertext to the reverse order of the coding process; every round consists of the four methods conducted in the reverse order –

- Add spherical key
- Combine columns
- Shift rows
- Computer memory unit substitution

Since sub-processes in every round are in a reverse manner, not like for a Feistel Cipher, the cryptography and decoding algorithms must be on an individual basis implemented, though they're closely related.

Data analysis and discussion

Let's see an example of AES-256-GCM stellate secret writing construction. For AES encryption, we will use a new python library known as pycryptodome, which supports this type of construction.

This type of construction takes input as a message and an encryption key, and as a result, it produces an output as a group of values present along with authTag. The nonce generated an initial vector (IV) for GCM construction in the ciphertext. The authTag is the message authentication code (MAC) calculated throughout the encryption [20-22].

Let us take a complex example for coding: AES encryption of text using a text password. We use the authenticated encryption construct AES256GCM, combined with the Scrypt key derivation.

Figure 4: Code for analyzing AES encryption.

During secretive writing, the Scrypt KDF derives a secret key from the password. The KDF is used during the decryption process and can be kept for encrypted messages. These input messages are basically the AES encrypted, which provides output containing authTag, ciphertext and IV, which is a random nonce.

The ultimate output holds these three values + the KDF salt, Figure 1.4. throughout the decryption, the Scrypt key derivation (with equivalent parameters) is used to derive the same secret key from the encryption password, along with the KDF salt (which was generated willy-nilly throughout the encryption). Then the ciphertext is AES-decrypted victimization, the essential key, the IV (nonce), and the authTag. In case of success, the result is decrypted original plaintext. And in case of error, the authentication tag can fail to attest the decoding method associated with an exception are thrown.

The output is given below, which may change due to randomness (as Figure 5).

Figure 5: The output of the previous code

Now let's look at the solution proposed in terms of protecting the data from attackers, which can also become a threat to cyberattack!!!

The above simulation figure 6, shows, however, the system will observe the user and wrongdoer and at a constant time can confuse an attacker, whereas having a secured secret key for the user to urge him to the target file and throw the attacker out of the system once the time gets over to access the system. Further, useful articles on cyber security and modern technologies for securing systems can be found in [20-45].

Figure 6: Flowchart depicting the entries of both attacker and user and their separate conditions.

Conclusion

In the course of this work, we have reached several conclusions. We understood what a password attack is, its types, and how we can use different methods to prevent each. We have proposed new ideas for protecting sensitive data from cyber-attacks in this work. Using the AES encryption method, we are creating a model in which the system can identify and mislead an attacker by using multiple password folders to further prevent the attacker from accessing the target file within a certain period., The user can directly use the private key to obtain the target file and increase the period to access the file. There can be different ways to use encryption to fight network attacks and become a threat to the hacker world! It's the responsibility of every individual to take all the necessary actions to secure their data. In case of attacks, measures should be taken accordingly to avoid being victimized.

Bibliography

1. S Zhang., *et al*. "A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity". in IEEE Access 8 (2020): 128250-128263.

2. N Floissac and Y L'Hyver. "From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion". 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography (2011): 43-53.

3. Ritambhara A Gupta and M Jaiswal. "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)". 2017 International Conference on Computing, Communication and Automation (ICCCA) (2017): 422-427.

4. L Yu., *et al*. "AES Design Improvements Towards Information Security Considering Scan Attack". 2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (2018): 322-326.

5. H Sun., *et al*. "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks". in IEEE Transactions on Information Forensics and Security 7.2 (2012): 651-663.

6. H R G Cacacho., *et al*. "Breaking the Password Security Standards Using Offline Attacks and Public User Attributes". 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM) (2019): 1-5.

7. C Routh., *et al*. "Attacks and vulnerability analysis of e-mail as a password reset point". 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ) (2018): 1-5.

8. E Sachdeva and S P Mishra. "Improving method of correcting AES Keys obtained from coldboot attack". 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (2015): 1-8.

9. G Yendamury and N Mohankumar. "Defense in Depth approach on AES Cryptographic Decryption core to Enhance Reliability". 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (2021): 1-7.

10. H. S. K. Sheth, I. A. K and A. K. Tyagi, "Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 476-485, doi: 10.1109/ICAAIC53929.2022.9793179.

11. Amit Kumar Tyagi, "Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era' Perspective: The Challenges and a Way Forward", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

12. Tibrewal I., Srivastava M., Tyagi A.K. (2022) Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_1.

13. Shabnam Kumari, P. Muthulakshmi, A Wide Scale Survey on Weather Prediction Using Machine Learning Techniques, Journal of Information & Knowledge Management, https://doi.org/10.1142/S0219649222500939.

14. Sheth, H.S.K., Tyagi, A.K. (2022). Mobile Cloud Computing: Issues, Applications and Scope in COVID-19. In: Abraham, A., Gandhi, N., Hanne, T., Hong, TP., Nogueira Rios, T., Ding, W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems, vol 418. Springer, Cham. https://doi.org/10.1007/978-3-030-96308-8_55.

15. A. Deshmukh, N. Sreenath, A. K. Tyagi and S. Jathar, "Internet of Things Based Smart Environment: Threat Analysis, Open Issues, and a Way Forward to Future," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, pp. 1-6, doi: 10.1109/ICCCI54379.2022.9740741.

16. F Skopik and S Filip. "Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators". 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (2019): 1-8.

17. Meghna Manoj Nair., et al. "Medical Cyber Physical Systems and Its Issues". *Procedia Computer Science* 165 (2019): 647-655.

18. Amit Kumar Tyagi and G Aghila. "A Wide Scale Survey on Botnet". *International Journal of Computer Applications* 34.9 (2011): 9-22.

19. Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137.14 (2016): 19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

20. G Rekha., *et al*. "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security". *Advances in Science, Technology and Engineering Systems Journal* 5.3 (2020): 72-81.

21. S Mishra and A K Tyagi. "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology". 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (2019): 123-128.

22. Amit Kumar Tyagi., *et al*. "AARIN: Affordable, Accurate, Reliable and Innovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology". *IJIN* 2 (2021): 175-183.

23. Amit Kumar Tyagi. Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World". *IGI Global* (2022).

24. Khushboo Tripathi., *et al*. "Comparison of reactive and proactive routing protocols for different mobility conditions in WSN". In Proceedings of the 2011 International Conference on Communication, Computing and Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA (2011): 156-161.

25. Jajula SK., *et al*. "Review of Detection of Packets Inspection and Attacks in Network Security". In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol 491. Springer, Singapore (2023).

26. Ranchhodbhai PN and Tripathi K. "Identifying and Improving the Malicious Behavior of Rushing and Blackhole Attacks using Proposed IDSAODV Protocol". *International Journal of Recent Technology and Engineering* 8.3 (2019): 6554-6562.

27. Midha S, Tripathi K, Sharma MK. Practical Implications of Using Dockers on Virtualized SDN". *Webology* (2020): 312-330.

28. D Agarwal and K. Tripathi. "A Framework for Structural Damage detection system in automobiles for flexible Insurance claim using IOT and Machine Learning". 2022 International Mobile and Embedded Technology Conference (MECON) (2022): 5-8.

29. S Midha., *et al*. "Cloud deep down — SWOT analysis". 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) (2017): 1-5.

30. K Somisetti., *et al*. "Design, Implementation, and Controlling of a Humanoid Robot". 2020 International Conference on Computational Performance Evaluation (ComPE) (2020): 831-836.

31. Sai GH., *et al*. "Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future". In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems (2023): 421. Springer, Singapore.

32. S Subasree., *et al*. "Combining the advantages of radiomic features based feature extraction and hyper parameters tuned RERNN using LOA for breast cancer classification". *Biomedical Signal Processing and Control* 72 (2022): 103354.

33. Kumari S and Muthulakshmi P. "Transformative Effects of Big Data on Advanced Data Analytics: Open Issues and Critical Challenges". *Journal of Computer Science* 18.6 (2022): 463-479.

34. Atharva Deshmukh, Disha Patil, Amit Kumar Tyagi, Arumugam S S, and Arumugam. 2022. Recent Trends on Blockchain for Internet of Things based Applications: Open Issues and Future Trends. In Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022). Association for Computing Machinery, New York, NY, USA, 484–492. https://doi.org/10.1145/3549206.3549289.

35. S Midha and K Triptahi. "Extended TLS security and Defensive Algorithm in OpenFlow SDN". 2019 9th International Conference on Cloud Computing, Data Science and Engineering (Confluence) (2019): 141-146.

36. Midha S and Tripathi K. "Extended Security in Heterogeneous Distributed SDN Architecture". In: Hura, G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering 668 (2021).

37. Midha S and Tripathi K. "Remotely Triggered Blackhole Routing in SDN for Handling DoS". In: Dutta, M., Krishna, C., Kumar, R., Kalra, M. (eds) Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India. Lecture Notes in Networks and Systems 116 (2019). Springer, Singapore.

38. Mapanga V., *et al*. "Design and implementation of an intrusion detection system using MLP-NN for MANET". 2017 IST-Africa Week Conference (IST-Africa) (2017): 1-12.

39. Tyagi AK. "Data Science and Data Analytics: Opportunities and Challenges (1st ed.)". Chapman and Hall/CRC (2021).

40. Tyagi AK and Abraham A. "Recurrent Neural Networks (1st ed.)". *CRC Press* (2022).

41. Tyagi AK and Abraham A. "Recent Trends in Blockchain for Information Systems Security and Privacy (1st ed.)". *CRC Press* (2021).

42. Kumar Tyagi A., *et al*. "Security and Privacy-Preserving Techniques in Wireless Robotics (1st ed.)". *CRC Press* (2021).

43. Tyagi A K., *et al*. "Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles". *IGI Global* (2021).

44. Tyagi A K. "Multimedia and Sensory Input for Augmented, Mixed, and Virtual Reality". *IGI Global* (2021).

45. Malik S., *et al*. "Impact and Role of Digital Technologies in Adolescent Lives". *IGI Global* (2022).