Cryptographic Compression Techniques along with some Penetrating Attacks and Possible Security Measures

Sobia Sattar^{1,*}, Shahan Yamin Siddiqui², Sana Mazhar³, Irfan Abbas⁴, Bilal Shoaib Khan⁵,
Abdul Hannan Khan⁶, Muhammad Sajid Farooq⁷

^{1,2,3,4,5,6}Department of Computer Science, Minhaj University Lahore, Lahore, Pakistan.

^{2,6,7}School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan.

⁴Department of Computer Science, University of Central Punjab, Gujrat, Pakistan.

^{1,*}Sobiasattar156@gmail.com,.

Abstract

Information security relates to protecting advanced secrecy unit that presents unapproved access to PCs, individual databases, and sites. Cryptography watches clients by giving utility to the mystery composing of information and affirmation of different clients. The need is to develop the techniques of lessening the number of bytes expected to speak to a provided arrangement of facts and figures. It licenses sparing a pile of learning. Organizations ensure information protection by using firewalls and mystery composing components. Cryptography is one of the best approaches to send and receive confidential information from one node to another. There are multiple data encryption systems available and AES is one of them. The data security framework contains privacy, quality, and respectability. In this article, we will embrace to imagine logical order of mystery composing, pressure and most absolutely varying sorts of assaults alongside fluctuated contrasting sorts of safety efforts that can be connected in venture with the prerequisite and style of the system.

Keywords: Cryptographic-Compression, Cryptographic-Concepts, Spoofing, Buffering, Anti-Malware.

1. INTRODUCTION

The compression is used for the protection of facts and figures, by utilizing this it uses fewer circle space (sets aside extra cash), massive information is exchanged over the

internet. It will expand the speed of learning exchange from plate to storage. Information security conveys learning insurance crosswise over big business. Information safety could be a developing issue among IT associations, all things t be considered.

To handle this developing concern, many IT organizations are shifting in the direction of cryptography to shield their important statistics [1]. Whereas higher than contemplations over anchoring hang on learning, IT associations additionally are confronting difficulties with consistently expanding to satisfy the association's present and future requests. Information pressure is comprehended for diminishing stockpiling and correspondence costs. It includes revising learning of a given arrangement, alluded to as supply message to information of a littler measured configuration alluded to as code word. Encoding is comprehended for protecting information from changes. It changes learning of a given configuration, alluded to as plaintext, to an alternate arrangement, alluded to as figure content, abuse relate degree mystery composing key. Cryptography means encryption of data. In vogue cryptography is vigorously upheld numerical hypothesis and connected science practice, logical control calculations are planned around process hardness suppositions, making such calculations difficult to hinder in pursue by any human. It's in principle feasible to hinder such a framework, anyway it's difficult to attempt in this manner by any distinguished sensible recommends that [2-3]. The extension of logical order innovation has raised an assortment of lawful issues inside the advanced time. Cryptography is a technique that is used for data safety. [3]. In this article, we will discuss different techniques, methods, and ways related to cryptography. Afterward, we will compare all ways with each other to find the best one and also find the limitations and advantages

of the system. We will discuss and compare all cryptographic compression techniques along with some penetrating attacks and possible security measures to improve the security of the data.

1.1 Cryptographic: Concepts and Objectives

People utilize PCs for managing an account, shopping, military, understudy records, and so on. Security might be of a fundamental issue in a few of those applications, we are in need to make sure that unrelate parties can't filter or alter messages [4].

1.1.1 Cryptography

The term cryptography has been derived from the Greek word "Kryptos", which depicts protected up, or "graphics" infers combining. The plaintext is the statistics which we want to identify, It's the main content, it may be in an extreme style of letterings, mathematical data, practicable projects, imageries, or the other very statistics, the plaintext, for instance, is that the causation of communication inside the source earlier than cryptography, or this one is the content at the accumulator once coding[4-5].

1.1.2 Cipher

To redesign plaintext to figure message, this technique is named coding, in various words, this is a component of changing decipherable and coherent facts into "inane" statistics. Computer security: This is a nonexclusive lexicon for a lot of devices intended to shield any statistics from programmers, burglary, defilement, or catastrophic event though permitting the

information to be offered to the clients at the indistinguishable time. The instance of those instruments is that the virus protection program [6].

1.1.3 Network Security

It alludes to any action intended to shield the convenience, respectability, irresponsibleness, and wellbeing of information all through their communication structure, Network security copes with equipment, and bundle. The effort might be one in all the ensuing enemy of contagion and hostile to spyware, protection by firewall, Interruption block structures, and VPN. Internet Security: These are actions and approaches won't shield learning all through their communication over a lot of interrelated systems, while data protection is concerning an approach to stop assaults, and to locate muggings on data-based structures [7].

1.1.4 Privacy

It is the first essential objective that assures that nobody will see the got information with the omission of the individual who is having the understanding key.

1.1.5 Authentication

It is the technique for representing the permission access. It proposes the client or the framework will determine their access to data as a user authentication goal [8].

1.1.6 Data Reliability

The unapproved data and material may get changed by partner, plan, or unintentionally. Credibility advantage

encourages that regardless of whether statistics are unharmed or not since. It might be proficient by abuse dicing at either side the sender and the benefactor to shape a novel communication procedure and contrast it and the one that got.

1.1.7 Non-Repudiation

The Non-repudiation component cannot determine that the despatcher increasingly communicates, and the communication was gotten by the ideal party, that the beneficiary cannot guarantee that the communication was not delivered. For occurrence, when a request is made, automatically a procurer cannot repudiate the procurement arrange, if the non-revocation benefit empowered amid this gathering activity [9].

1.1.8 Access Control

It is the strategy for avoiding partnered unapproved utilization of assets. This objective controls the UN office will approach the assets if one can access underneath that boundaries and circumstances the entry will have occurred, and what is the authorization dimension of an assumed admittance.

2. LITERATURE REVIEW

There are a lot of different methods, techniques, and approaches to encrypt data. There are some data encryption ways use for encryption and decryption which we are focusing on.

2.1 Data Encryption

A learning coding could be an arbitrary bit collection prepared clearly to

clamber and unraveling statistics. Encryption is implied with intentions proposed to ensure that every mystery's capricious and unmistakable. Cryptography utilizes two sorts of keys: symmetrical and uneven. Symmetrical keys are round the longest; they use one key for each the coding and mystery composing of the figure content. This kind of mystery's alluded to as a mystery key. Mystery key figures regularly involve one among two categories: stream figures or square figures [9]. A square figure applies a non-open key and recipe to a square of data in the meantime, while a tributary figure put on the key and equation one piece at any given moment. Extreme cryptologic procedures utilize symmetrical coding to encode learning transmissions anyway utilize uneven coding to encode and trade the key. Symmetrical coding also alluded to as close to home key coding, utilizes consistent individual key for each coding and mystery composing. The peril amid this framework is that if whichever party fails the key or the mystery blocked, the structure is wrecked and communications cannot be altered immovably [10].

2.1.1 Symmetric-Key-Encryption

Isosceles key cryptography is furthermore alluded to as Private-key cryptography, a Mystery-key is likewise controlled by one individual or changed among the dispatcher and the recipient of information. On the off chance that non-open key-cryptography is utilized to dispatch mystery information between two parties, each the despatcher and beneficiary must have a replica of the key [10].

Figure 1: Symmetric cryptosystem

2.1.2 Asymmetric-Key-Encryption

This framework defines the key management (public), the first key encodes the statistics and additional mathematically associated key decodes it. Pc which is causing Associate in nursing encoded message utilizes a chose non-open key that is pooled and after that is thought exclusively to the dispatcher. On the off chance that a causing workstation introductory encrypts the information with the alleged beneficiary's open key and again with the despatcher's mystery, non-open key, At that point, the accommodating PC could disentangle the information, starting exploitation its mystery key thus the despatcher's open key. Consuming this open key logical order procedure, the dispatcher and receiver region unit ready to show each other further as shield the mystery of information [10-11].

Figure 2: Asymmetric cryptosystem

2.2 Compression

Compression calculations cut back the repetition in statistics representation to reduce the volume compulsory for that

learning. Throughout the latest period, there has been an Associate in Nursing exceptional blast inside the amount of progressive learning communicated utilizing the web, talking to content, images, movie, sound, workstation agendas, and so forth. Statistics burden infers causation or putting away a little scope of minutes. The pressure is that the decrease in dimensions of information as to spare heaps of territory or TRM as shown in figure 3[11].

Figure 3: Compression Technique

3. METHODOLOGY

Different cryptographic methods are used all around the globe to provide benefits to the persons and different organizations want to secure data from different attacks. Took the data from different articles to evaluate different features and measures like compression techniques, penetrations attacks, all possible measures. Now for verification, the data has been organized and we can easily analyze. We have obtained data to analyze and predict the best way. To better understand the dynamics of the different security measures and attacks, we first extract the useful data. We filter the data by different compression techniques, security measures, and attacks to get more accurate systems for the safety of the data.

Many ideas are working in different

countries and platforms every system is different from the other according to the different features, procedures but still people and organizations face many issues.

Methodologies are utilized for two general classes, Lossy, and lossless techniques. Lossy Compression typically utilized to pack an image. amid this unique learning is anything but a twin of compacted information which implies there's some misfortune e.g. Square Truncation mystery composing, revamp mystery composing, and so forth lossless Compression utilized for pack any issue in the process of learning

4. ATTACKS

Systems territory unit focus to assaults consequent to malware (vindictive) causes. Furthermore, with the appearance and expanding utilization of net connect is usually on the rise and increasing day by day. Majorly two classifications are considered for these attacks namely: "Aloof" (in which an unwelcome individual system is being captured by the host system going through it) and "Dynamic" in which an unwelcome individual interferes with the customary activity of a system to disturb the system. To restrict hurt and recuperate, a 'framework' is developed rapidly once assaults happen. Their zone unit is located somewhere in the range of a ton of various physical malware attacks which is basic to be contemplated [12-13].

4.1 *Passive Attack*

An inactive assault examines the decoded circulation plus appears

against 'touchy data' and 'secure-content passwords' that can be used in several classes of assaults. Whereas, tuning in or recognition of channel with an unapproved assailant's square measure referred to latent assault. It includes traffic screening, recognizing unprotected correspondences and unscrambling weather-beaten scrambled traffic, and catching verification data like passwords. Aloof block attempt of system activities grants enemies to test moving toward activities. Inactive assaults result in the noteworthy of data or data records to scholastic degree transgressor rather than assent or client's information [14, 15].

4.2 Active Assault

In a fiery assault, the assaulter endeavors to sidestep or constrained the bolt anchored-frameworks within an 'event correspondence'. This must be feasible by Trojan steeds, infections, hiding, or worms. Dynamic assaults typify endeavors to present the noxious code, to change or take the information, and to stay away from or break security alternatives. Unapproved assailants examine, tune in, and changes information stream within a line territory unit referred to as a dynamic assault. These physical malware attack zone units are mounted for a system spine, electronically infiltrate associate (in the nursing area), abuse information in travel or assault an authorized remote client by targeting the join to associate within a nursing locale. A dynamic assault leads to confession or scattering of data records, change of data, or denial of service [16].

4.3 Distributed Assault

Similar to a bug or secondary passage sequencer, to a believed constituent or programming bundle which will be disseminated later to a few elective firms and consumer's circulation; change of apparatus or software design bundle at the modern plant or all through conveyance. These pastings present malignant codes like indirect access to an item to a framework work in the future or to acknowledge an unapproved admittance towards statistics. [14, 17]

4.4 Insider Assault

Studying insider we observed to be the reason in 21% of safety ruptures, because of the activities of insiders, 21% further has been found. The greater part of defendants to additional ongoing review said it is progressively troublesome today to recognize and counteract insider assaults and 53% were expanding their sanctuary safety plans because of insider dangers. While a noteworthy assortment of ruptures is caused by pernicious or discontent specialists - or previous laborers - a few are caused by good-natured specialists World Health Organization are simply endeavoring to attempt and carry out their responsibility. BYOD projects and record sharing and joint effort administrations like Dropbox imply that it'll be stronger than any time in recent memory to remain organization data underneath organization the executives inside the substance of those benevolent anyway trigger-cheerful specialists.

A nearby in assault includes someone endeavoring to ask physically close

system components, information, and frameworks to discover a great deal of two or three systems. Shut-in assaults contain standard individuals accomplishing close somatic nearness to systems, framework, or offices for the point of altering, assembling, or negating admittance to facts. Amid a societal designing assault, the assailant bargains the system or framework through societal communication with a person, via partner degree email information or telephone. Changed traps will be used by the person to uncovering information concerning the wellbeing of the organization. The information that the unfortunate casualty uncovers to the programmer would potentially be utilized in a future assault to accomplish unapproved access to a framework or system [18].

4.5 Close-in Attack

An unaffected PC safety risk, spyware somewhat packages that shades your on-line workouts or familiarizes programs though not your acquiescence for advantage or to catch distinct material. This data is malignantly applied because of the authentic client for that exact reasonable work [19].

4.6 Spyware Attack

In Phishing assault, the programmer makes an imagined net informatics framework that appears to explicitly type of and a mode site simply like the SBI bank or PayPal. Associate in having email communication endeavoring to snare the client into snapping a connection that winds up in the imagine net electronic PC. When the client activities to go on-line with their material, the computer operator

registers the id and word hence attempts that information on the \$64000 net electronic PC [20].

4.7 Phishing Assault

A computer operator adopts control over a period among you an alternative person and separates the elective person from the correspondence. You keep on being that your territory unit addresses the essential party and may dispatch individual facts to the programmer by unintentionally [21].

4.8 Spoof Assault

The programmer adjusts the supply of addresses to the person which is causing harm all together; that they appear to come back from another person. It can be an undertaking to sidestep your firewall documentation.

4.9 Password Assault

A miscreant endeavor to split the code word or password keeps in an extremely organized data or a secret phrase ensured record. There are 3 noteworthy sorts of Arcanum assaults: a word book assault, a beast compel assault, and a half and half assault. A wordbook assault utilizes a thesaurus record that could be a rundown of potential passwords [21-22]

4.10 Buffer Excess/Overflow

A support flood assault ordinarily prompts the aggressor picking up body access to the framework in an exceedingly incite or casing.

4.11 Exploit Assault

In this type of assault, the miscreant aware of protection disadvantages at interims a product framework or a lump of programming framework and uses that data by abusing the defenselessness.

5. NETWORK SECURITY TECHNOLOGIES

Web hackers can be a noteworthy problem inside the world as long as facts are available and exchanged over the net. Entirely unexpected barriers and discovery instruments were produced to take into account assaults referenced before. Some of these systems together with development thoughts are noticed amid this area [23].

5.1 Cryptographic Systems

Cryptography is helpful and used for abstraction or protection. It comprised the consumption of specific symbols and statistics to the transformation of data into meaningful information.

5.2 Firewall

The firewall could be a run of the mill fringe the executive's instrument or border safeguard. The point of a firewall is to dam traffic from the surface, anyway, it may even be acclimated square commuter traffic from a private insider. It is a protection line or layer in contradiction of gatecrashers to get inside the framework. It is a framework intended to prevent unapproved entrance into an individual system. Firewalls are authorized in every equipment and PC code [16, 23].

5.3 Pouring Security to the Hardware Level

To more streamline execution and increment data protection, Intel creates stages furthermore epitomizes numerous correlative security advancements built into different stage parts, together with the super-computer, chipset, and organize interface controls. These innovations offer low-level building obstructs upon that a protected system foundation will be continued. These advancements exemplify Virtualization Machinery, trusty Execution Equipment.

5.4 Intrusion Detection Systems(IDS)

IDS structures are regularly software design frameworks and tools acclimated to discover an assault. IDS items are acclimated screen relationship insignificant regardless of whether assaults are being pushed. The standard antivirus stock refers to the interruption discovery framework [18, 24]. Framework's acclimated monitor the hazardous items phenomena are named formerly as 'interruption recognition frameworks'. Detecting interruption in an organization and government setup units might be an obtrusive field of security inspection and the mentioned development has been provoked through determination which is a lot of frameworks that make no viable utilization of record and review learning.

5.5 Anti-Malware Software and Scanners

Infections, worms, and Trojan ponies are for the most part instances of

pernicious software design, or Malware, for small. Exceptional termed anti-Malware gadgets are consumed to differentiate them and fix an adulterated structure.

5.6 *Secure Socket Layer (SSL)*

The SSL could be a collection of resolutions that is a standard on account of succeeding a legit dimension of safety concerning a web platform and a site. It is planned to frame a safe opening among net, a web, an online platform and subsequently the network server, all together that any information changed is guaranteed between the anchored passages. It gives endorsement of customers on servers over the use of testaments. [21-24]

5.7 *Dynamic Endpoint Modeling*

Recognizable safekeeping reply speaks to extremely new on account of watching IT security. It shows each gadget on your system, in this way you'll have the capacity to see customary conduct and rapidly make a move once an apparatus begins acting unusually. There isn't any must introduce operators on the gadgets, or attempt and utilize profound bundle audit, furnishing you with a strong response to beat these new security challenges.

6. NETWORK POLICY MEASURES

6.1 *Making a Secure Cloud Environment*

Experts show that with the help of the secure cloud, useful information and data can be locked. It can only be

accessed by the authorized administrators having the security keys for the block chained cloud present inside a network which will be further helping in distributed computing cloud situations. This also gives us the job-based security arrangements over the network.

6.2 *Implementation of Zero Trust Mechanism*

This type of mechanism is having a strong concept of public-key cryptography for making the users over the network to communicate with all the logical key concepts to achieve a strong level of security. There are checks which are encrypted in the format and structure of the frameworks which are taking part in the communication of the data over the network. Conceptual information security is displayed vitally with the applications of (ZTM) zero trust display situations.

Computational Acumen methods like Fuzzy logic [22,24-26], Swarm Intelligence [26,28] Deep Extreme Learning Machine [28-29], Neural Network [27-28,30], & like Genetic Algorithm [30], Differential Evolutionary (DE), Island GA [30], Evolutionary Computing [29-31] are strong contender solutions in the field of smart city [26-29, 32], Smart health [26, 28,32] , smart energy [33], wireless communication [34] as well as Cryptography [31] etc. Computational Methods are hot research area which is also used in zero trusted mechanism.

6.3 *Administrative Services for Trend Micro Threads*

The method for information protection for network administrators which are

attacking the network over the process of data communication. They check the URL and trends of micro threads and immediately block them if they are checking the security layer protocols of the communication framework of the layer [31]. They provide a secure environment and make understandings of the loopholes in the network and make them administer all the vulnerabilities which are affecting the network of the domain. Many organizations are using these real-time services for making their network the most secure network in terms of data loss and micro threads protections [32].

7. RESULTS AND DISCUSSION

Security could be horrendously extreme and essential. Major build system use for better security and data protection. All types of security attacks are discussed in detail. Multiple types of attacks are discussed. Multiple compression ways are also discussed as well as different network policy measures and network security technologies are discussed. After sketched out the security purposes, endeavors happening inside the system are assessed by pertinence that approach. In this way, at every point, we highlight the advantages and problems that the user's face. The current context will in general attempt to audit these extraordinary assortments of attacks that intrude our structure. The protected application of our structures and net there are fluctuated extraordinary safety arrangements are generating. In this paper, we have noticed the approaches which will be utilized to a great extent by several clients and a couple of new progress physiognomies that matches

today's circumstances such as utilizing tremendous data characteristics in security provision, Trend little security system and so on. Security is exclusive with everybody's participation and everyone's the same old thing, Associate in a nursing shrewd arrangement, and reliable practices can be feasible. In the end, in every point we defined which system has some issues and which one is best according to the penetration attacks, security attacks, security policies, security measures, and security systems for the benefits of the organizations. Symmetric and asymmetric key encryption is the types of AES methods that protect 256 bits of data at one time. Insecurity attacks Password-Assault-(PA) is the most protect algorithm. Administrative services for trend micro threads is the best network policy measures, as well as cryptosystem, is a good technique for data protection.

8. CONCLUSION

Cryptographic systems are applied to guarantee that the constituent of communication are privately communicated and cannot be altered. Classification proposes that not a single person will see the acknowledged information aside from the individual who is having the translate key, and "information shall not be adjusted. Cryptographic systems can make network security more accurate and timely with the help of symmetric and A-symmetric cryptosystems. Dynamic endpoint modeling and compression along with symmetric key cryptography initiates the most well-known secure network for the data characteristics which are needed to be sent over a secure network. Many organizations

are following these secured modeling concepts. In some penetration attack compression techniques are also helpful in achieving best-layered security. Firewall and SSL systems can also help the network to achieve the smartest technological secure environment for the smooth flow of information and useful datasets.

REFERENCES

- [1] Bjorn, V. (2000). U.S. Patent No. 6,035,398. Washington, DC: U.S. Patent and Trademark Office.
- [2] Youngblood, G. (2020). Expanded cinema. Fordham University Press.
- [3] Gurunathan, K., & Rajagopalan, S. P. (2020). A steganovisual cryptography technique for multimedia security. *Multimedia Tools and Applications*, 79(5), 3893-3911.
- [4] Sprenger, T. (2020). U.S. Patent No. 10,630,474. Washington, DC: U.S. Patent and Trademark Office.
- [5] Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal Of Engineering And Computer Science*, 6(4).
- [6] Dhankani, M., Dhameja, A., Darda, S., & Bohra, D. (2015). Anonymous communication system based on onion routing. *International Journal of Computer Applications*, 121(23).
- [7] DEVI, A. (2018). Network Security and Cryptography. Journal Homepage: <http://www.esrjournal.com> Email: esrjeditor@ gmail. com, 6(4).
- [8] Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal Of Engineering And Computer Science*, 6(4).
- [9] Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal Of Engineering And Computer Science*, 6(4).
- [10] Almazrooie, M., Samsudin, A., Gutub, A. A. A., Salleh, M. S., Omar, M. A., & Hassan, S. A. (2020). Integrity verification for digital Holy Quran verses using cryptographic hash function and compression. *Journal of King Saud University-Computer and Information Sciences*, 32(1), 24-34.
- [11] Singhal, S., & Pathak, H. Cryptography Based Hybrid Security Architecture for Mobile Multi Agents. *International Journal on Recent and Innovation Trends in Computing and Communication*, 4(11), 154-159.
- [12] Branche, P. O. (2017). Ransomware: An Analysis of the Current and Future Threat Ransomware Presents (Doctoral dissertation, Utica College).
- [13] Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal Of Engineering And Computer Science*, 6(4).
- [14] Gaigole, M. S., & Kalyankar, M. A. (2015). The study of network security with its penetrating attacks and

possible security mechanisms. *Int. J. Comput. Sci. Mob. Comput*, 45(5), 728-735.

[15] Gaigole, M. S., & Kalyankar, M. A. (2015). The study of network security with its penetrating attacks and possible security mechanisms. *Int. J. Comput. Sci. Mob. Comput*, 45(5), 728-735.

[16] Ahmad, A. (2012). Type of security threats and its prevention. *International Journal of Computer Technology and Applications*, 3(2), 750-752.

[17] Turab, N. M., Taleb, A. A., & Masadeh, S. R. (2013). Cloud computing challenges and solutions. *International Journal of Computer Networks & Communications*, 5(5), 209.

[18] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*.

[19] Shabbir, A., Khan, H. R., Ali, S. A., & Rizvi, S. (2016). A Stochastic Geometrical Approach for Performance Analysis of Heterogeneous Cellular Network. *International Journal of Computer Science and Information Security*, 14(8), 467.

[20] Adeyinka, O. (2008, May). Internet attack methods and internet security technology. In *2008 Second Asia International Conference on Modelling & Simulation (AMS)* (pp. 77-82). IEEE.

[21] Al-Garadi, M. A., Mohamed,

A., Al-Ali, A., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*.

[22] Drake, C. N. T. (2020). U.S. Patent No. 10,574,692. Washington, DC: U.S. Patent and Trademark Office.

[23] Hussain, S., Abbas, S., Sohail, T., Adnan Khan, M., & Athar, A. (2019). Estimating virtual trust of cognitive agents using multi layered socio-fuzzy inference system. *Journal of Intelligent & Fuzzy Systems*, 37(2), 2769-2784.

[24] Areej Fatima, Muhammad Adnan Khan, Sagheer Abbas, Muhammad Waqas, Leena Anum, and Muhammad Asif, Evaluation of Planet Factors of Smart City through Multi-layer Fuzzy Logic (MFL). *The ISC Int'l Journal of Information Security*. 51-58, 2019.

[25] Siddiqui, S. Y., Hussnain, S. A., Siddiqui, A. H., Ghufuran, R., Khan, M. S., Irshad, M. S., & Khan, A. H. (2019). Diagnosis of Arthritis Using Adaptive Hierarchical Mamdani Fuzzy Type-1 Expert System. *EAI Endorsed Transactions on Scalable Information Systems*, 19(18), 1-16.

[26] Atta, A., Abbas, S., Khan, M. A., Ahmed, G., & Farooq, U. (2018). An adaptive approach: Smart traffic congestion control system. *Journal of King Saud University-Computer and Information Sciences*.

[27] Khan, M. A., Umair, M., Saleem, M. A., Ali, M. N., & Abbas, S. (2019). CDE using improved opposite based swarm optimization for MIMO

systems. *Journal of Intelligent & Fuzzy Systems*, 37(1), 687-692..

[28] Ali, M. N., Khan, M. A., Adeel, M., & Amir, M. (2016). Genetic Algorithm based adaptive Receiver for MC-CDMA system with variation in Mutation Operator. *International Journal of Computer Science and Information Security*, 14(9), 296.

[29] Umair, M., Khan, M. A., & Choudry, M. A. S. (2015, December). Island genetic algorithm based MUD for MC-CDMA system. In 2015 International Conference on Information and Communication Technologies (ICICT) (pp. 1-6). IEEE.

[30] Umair, M., Khan, M. A., & Choudry, M. A. S. (2013, January). GA backing to STBC based MC-CDMA systems. In 2013 4th International Conference on Intelligent Systems, Modelling and Simulation (pp. 503-506). IEEE.

[31] Kashif, I., Muhammad, A.K., Sagheer, A., Zahid, H., & Areej, F (2018). Intelligent Transportation System (ITS) for Smart-cities using Mamdani Fuzzy Inference System, *International Journal of Advanced Computer Science and Applications (IJACSA)*. ISSN: 2158-107X, Vol. 9, No. 2, (pp. 94-105), Digital Object Identifier (DOI): 10.14569/IJACSA.2018.090215.

[32] Abbas, S., Khan, M. A., Falcon-Morales, L. E., Rehman, A., Saeed, Y., Zareei, M., & Mohamed, E. M. (2020). Modeling, Simulation and Optimization of Power Plant Energy

Sustainability for IoT Enabled Smart Cities Empowered with Deep Extreme Learning Machine. *IEEE Access*, 8, 39982-39997.

[33] Asif, M., Khan, M. A., Abbas, S., & Saleem, M. (2019, January). Analysis of Space & Time Complexity with PSO Based Synchronous MC-CDMA System. In 2019 2nd international conference on computing, mathematics and engineering technologies (iCoMET) (pp. 1-5). IEEE.

[34] Asadullah, M., Khan, M. A., Abbas, S., Alyas, T., Saleem, M. A., & Fatima, A. (2020). Blind Channel and Data Estimation Using Fuzzy Logic Empowered Cognitive and Social Information-Based PSO. *International Journal of Computational Intelligence Systems*, 22(1), 1-9.