IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Brief Review Of Cryptography Techniques For The Cloud Data Security

Pushpendra Tiwari[1]
Research Scholar,
Dept. of Computer Science, Madhanchal Professional University, Bhopal.

Dr. Md. Vaseem Naiyer[2]
Assistant Professor,
Dept. of Computer Science,
MadhanchalProfessonal University, Bhopal.

Abstract:

Today's time is completely of cloud computing, internet etc. Under which the role of cryptography is prominent in the exchange of digital content. With the help of cryptography, data can be encrypted and decrypted in different types of applications. The literature related to cryptography has been reviewed under the presented research paper, which makes it clear in which directions research work can be presented in various traditional cryptographic fields. Here various algorithms built on cryptography are explained in detail. After analysing the algorithms currently used in cryptography, new algorithms can be proposed to solve the problems found.

Keywords: Cryptography, Cloud computing, algorithms, Data Security etc.

I. Introduction:

Today's era is the era of technology. Today we are surrounded by technology from all sides. All our day-to-day work is also being done with the help of technology. In this era, various types of information are being sent and received through technology. The confidentiality and security of information sent through technical means is an important task. Which decides whether the information sent is not being used or intercepted by any third or other person. From the point of view of privacy and security, cryptography technology is used to secure the information being sent by technology. Cryptography technology is a technique through which secrecy is provided to any type of digital information. The traditional and more fundamental problem of deciding the security of information through this is to provide secure communication over insecure media, thereby providing security to the communication by a third party. Cryptography is the study of such science and mathematical methods, in which information is specially protected. The basic purpose of cryptography techniques is to protect confidential information by hiding large random binary sequences. With the help of these random sequences, the privacy and balancing

properties are secured. RNGs are used in a variety of applications such as cryptography, signature analysis, estimation of immunity to noise ratio of digital systems, testing of physical, electrical and biological systems such as code density testing, Volterra Kennel and Wiener in nonlinear systems Determination of, artificial neural network etc.

Due to technological development and utility of internet, there has been a substantial increase in digital content. To maintain the security of these digital contents, the international data encryption algorithm, advanced encryption slandered, a linear feedback shift register, and linear congenital generator are unsuitable for encryption and decryption of data due to the strong correlation between image pixels. Therefore, there is a need to generate high randomness and large volumes of digital content due to the high demand for input in random sequence for the wide variety of applications available in the market. Therefore, this random sequence determines the security strength of the cryptosystems. This emerging internet world as well as other applications related to avionics communication, bank transactions, financial markets, etc. require high level of network security and enable hardware architecture to be implemented to handle this sequence, through which the private key can be made available to the public for effective data cryptography. It is widely used in cryptography for key generation, encryption/decryption Internet gambling and masking protocols.

II. **Cryptography**:

The technique of cryptography is a technique with the help of which data is protected from being accessed by unauthorized persons or users. In fact, there are mainly two components in cryptography. The encryption technique is seen as the first component and the key as the second component. In this whole scenario, the key is applied to complete the encryption process depending on the type of algorithm used to encrypt. Many algorithms namely DES, AES, TDES, and RSA are available in this direction (William Stallings, 2013)

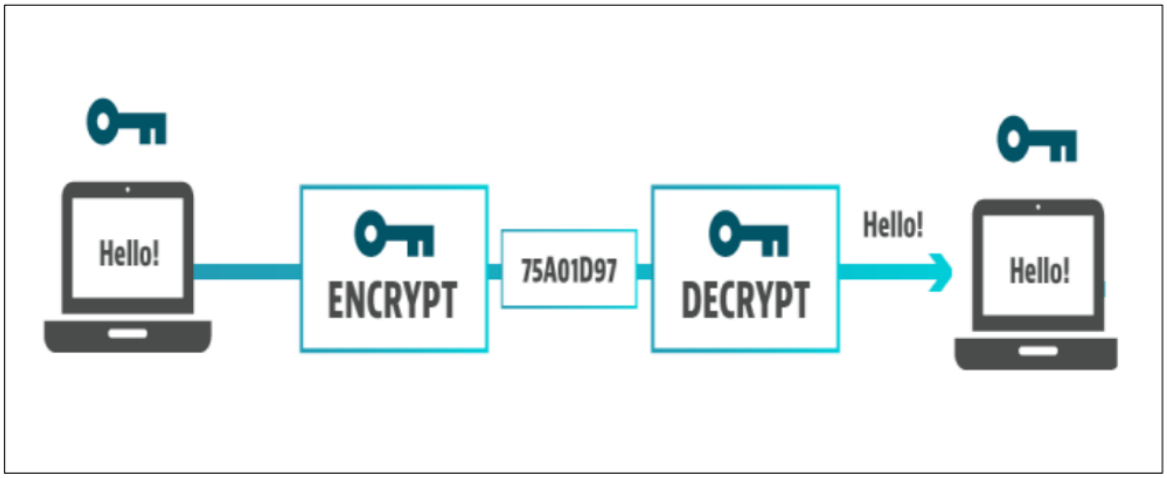
The strength of any cryptography based encryption technique depends on the strength of the key. In addition, the work is accomplished by incorporating key customization processes focusing on security objectives such as confidentiality, data integrity, and authentication. A longer key value takes more computation time to crack the source code, making it more difficult for hackers to trace the key. Therefore, key generation, key exchange and rekeying techniques have emerged as major research challenges in cryptography.

Cryptographic techniques are mainly classified into two classes, first is: symmetric key-based encryption algorithms and second is: Asymmetric key based cryptographic algorithms. Symmetric key-based encryption algorithms is one such algorithm, in which the key value is very useful for encrypting the message, which is similar to the key value and decrypts the data, and Asymmetric key based cryptographic algorithms is one such algorithm, In which different key values are used to carry out the encryption as well as decryption processes. It is also called public key cryptography. If both are studied comparatively, it is concluded that instead of symmetric key-based encryption algorithms, Asymmetric key based cryptographic algorithms are successful in working faster.

Cryptography is essential for providing data security for all types of organizations while on the other hand it is also successful in ensuring the privacy of authorized individuals. Now-a-days, very little trust is being shown by individuals on passwords and their data as all kinds of passwords or data are getting hacked by hackers. Even though many symmetric key cryptographic algorithms including Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (TDES), RC2, and RC6 are available for encryption, they were analysed by attackers and keys were inferred. Therefore asymmetric cryptography algorithms are also called public cryptography as it includes Diffie-Hellman Algorithm, RSA, and Digital Signature Algorithm etc. to strengthen the security approach. These algorithms have been developed to protect these cryptographic algorithms from specific types of attacks. Traditionally, cryptographic mechanisms such as authentication and encryption can be used to solve security problems in WSNs.

Cryptographic attacks are mainly classified into two categories, namely system attack and data attack. Here system attack is a special type of attack which attacks the flow of data from the source node which is identified by the network. Furthermore, attacks are classified into four types based on their application behaviour, such as interruption, interception, modification and fabrication attacks. Interruption attacks focus on attacks on networking-based resources that perform the task of passing information from a source node to a destination node whenever transmission becomes unavailable on a data server.

Interception type attack is the next type of attack which focuses on breaking the confidentiality of any system. On the other hand, modification attack is another type of attack which focuses on breaking the data integrity during transmission. Ultimately, a data attack is performed while analysing the crypto on the cipher text. In cryptographic attack, this type of algorithm is classified into four types namely cipher text-only type of attacks, the known plaintext based attack, an attack using a chosen-plaintext, and finally the attack based on the chosen cipher text. These cryptographic attacks can be detected by implementing various security algorithms anticipated by various researchers. Therefore, in this situation, it is necessary to develop a new security system through steganography and cryptography. The complete process of cryptography can be understood through the following diagram:



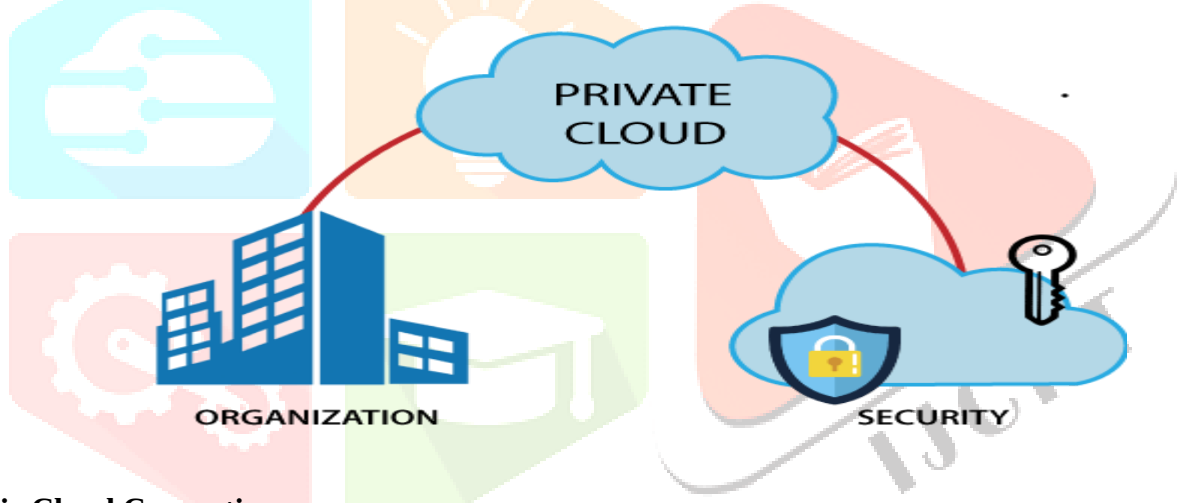
III. Cloud Computing:

In the present era, with the help of internet, we are able to complete important tasks sitting at home with great ease and alertness. In which the role of cloud computing is also important. With the help of cloud computing, the user can upload any type of information or digital data to the server and can also access it with the help of a remote server. We can store any kind of digital data on the server without using our personal storage device. In today's time, cloud computing has emerged as a great tool for common users and businessmen. Using this, time, cost etc. can be easily saved and productivity can be increased. With the help of internet, the facility of cloud computing can be obtained.

Types of cloud computing: Following are the four types of cloud computing that you can deploy as per the needs of the organization:

1. **Private Cloud Computing**:

Private cloud computing is a technology that creates an environment that represents an end user or group. Normally this environment works behind user and required group firewalls. With the help of this technology, the IT infrastructure is segregated from the public and limited to a single customer. It is used by various organizations and other parties to build and manage individual data centres.



2. **Public Cloud Computing**

Public cloud computing technology simply creates an environment in which an IT infrastructure is structured in such a way that users can access any type of facility publicly. In this type of technology the ownership is not vested in the end user. Some companies that provide services as a public cloud include Alibaba Cloud, Amazon, Google Cloud, etc.

Traditionally, the public cloud in use was always run in an off-premises mode, but with this type of technology, providers have started offering cloud services through on-premises data centres. . The distinction of location and ownership of their data centres has been done away with. When the cloud environment is partitioned, all other types of clouds become public clouds. Public cloud services can now be accessed for free as well. The IT infrastructure used by public cloud providers is sold and developed on a certain platform only.

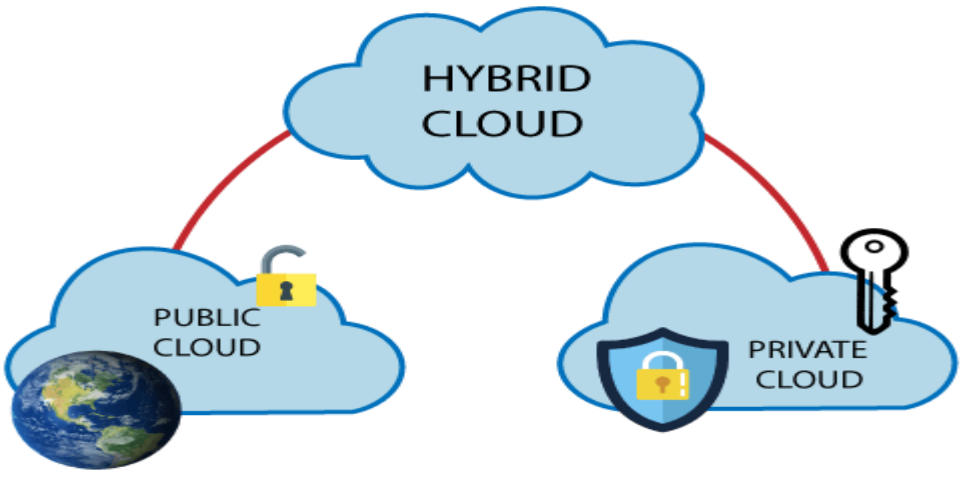
3. **Hybrid cloud computing**

Both private and public types of cloud computing are used together in a hybrid form. This type of cloud computing is considered secure in part because the services being publicly provided can be accessed by anyone publicly. Only individuals working on the same organization can access the services on a private cloud server. When different types of apps keep changing from the cloud server, then such server is called hybrid cloud.

Under Hybrid Cloud Computing, the following types of combinations are used:

1. One Private Cloud and One Public Cloud
2. One Private Cloud and One Private Cloud
3. One Public Cloud and One Public Cloud
4. More than one private and more than one public cloud

Cloud computing created by combining all the four types mentioned above is considered under hybrid computing. From this it is becoming clear that private cloud and public cloud can be used together, which is capable of providing a measurable result. Hybrid type of cloud computing has become the most commonly used server today. This type of cloud server is bound to increase in the future.



4**. Community cloud computing**

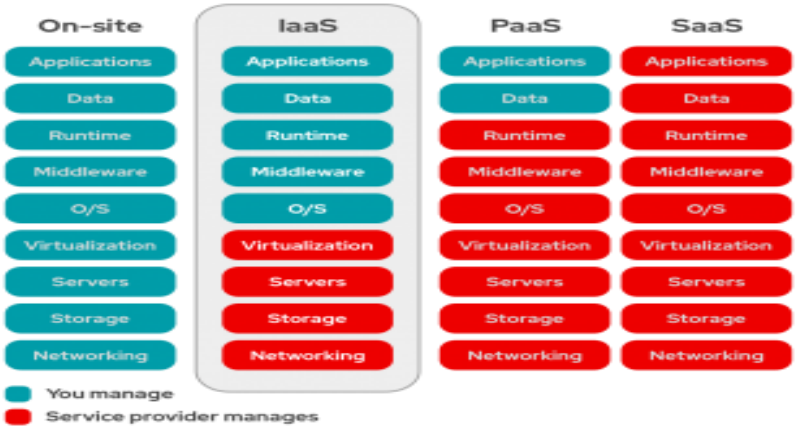
Community cloud systems are systems that allow the sharing of knowledge between specific groups of a variety of organizations and within a specific group. Servers are owned, managed and operated by a single organization, community or combination of third parties. A community cloud system provides a type of shared cloud computing service environment that is targeted to a certain number of organizations or employees. Eg: bank, business, form etc. Example: Health Care community cloud.

IV. Cloud services:

There is a definite structure to make cloud computing publicly available to the end user, through which all types of cloud related facilities are made available. It includes cloud computing infrastructure, platform and software, which is provided by the server provider with the help of internet. Here all types of elements of front end and back end used by cloud computing are explained in detail. The services used in front end and back end are mainly classified as follows:

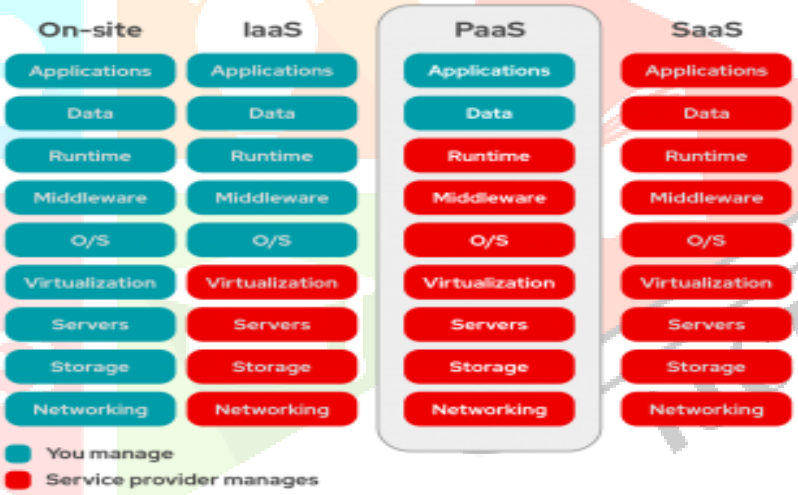
1. **IaaS**

IaaS refers to a cloud service provider that refers to infrastructure management. That is, an infrastructure that includes providing space on servers, managing the network, providing virtualization functions, etc. with the help of the Internet. Cloud computing users are limited to IP addresses or dashboards obtained from their devices by paying through a service provider to access infrastructure on servers. Here the user manages various things like operating system; apps and middleware etc. whereas the provider manages hardware, networking, hard drives, storage data and servers and manages all kinds of hardware related issues. It takes special care of cloud storage providers.



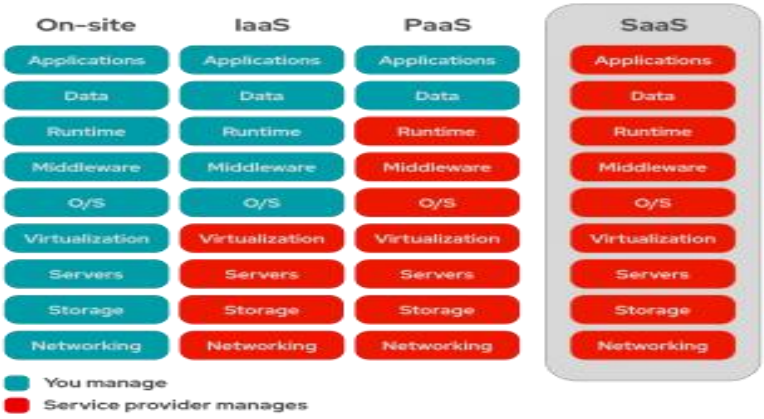
2. **PaaS**

PaaS is a service that manages both software and hardware. That is, under this, the platform of on-demand infrastructure, hardware, software development tools is made available. Under this, the work of running, developing and managing the related program is completed without any complexity and cost. It is mainly the application developed by the programmer or apps developer and the associated hardware both are shared together in a single platform. It is mainly used to build and maintain infrastructure.



3. **SaaS**

SaaS refers to a service that provides application software to the user. With its help, the management of cloud computing is done by the service provider. Simply put, SaaS is a service that is used through web applications or mobile apps. This facility is accessed through a web browser. Here the pupation of software, maintenance of any kind of error etc. is done for the users. Here the web application or mobile application connects to the dashboard or through IP. It saves the work of installing on an individual computer and provides ease of maintenance by a group and team.



V. Literature Review:

Susan et al. [4] it was told that under the subject of computer science, network and computer security is a new and very fast moving technology, with the help of which computer security education is a major goal. Various aspects such as hashing techniques, encryption, and security courses are majorly focused on the algorithms and mathematics to implement it. As crackers find ways to hack network systems, new courses are created that cover the latest types of attacks, but each of these attacks becomes out-dated daily due to the responses from new security software. To make security technology more robust, it is necessary to continuously upgrade security skills by driving business maturity, network optimization, security architecture and tweaking legal stakes.

Othman O. Khalifa et al. [5] clearly described the primary infrastructure, key features, and main goals of cryptography. He also clarified that in the current times i.e. in the age of information technology, communication has played a vital role in contributing to the development of technology. This has made it clear that there is a need to protect and assure the confidentiality of data sent through communication.

NitinJirwan et al. [6] clarified that data communication is mainly done in digital form. Data security is given top priority with the help of the use of encryption algorithms in this digital form so that the data can be safely accessed and delivered to the user without any issues. To accomplish this task, cryptographic techniques are also demonstrated which prove useful in the process of data communication, such as symmetric and asymmetric methods.

SandeepTayal et al. [7] presented a critical study on network security and cryptography, noting that with the emergence of social networks and commerce applications, a large amount of data is being generated around the world. This makes the security of information a major issue in terms of ensuring absolutely guaranteed data transfer with the help of servers and the web. Demonstrate the need for cryptographic techniques for the simultaneous use of a large number of users with the help of the Internet.

Anjula Gupta et al. [8] a detailed description of the origin, practice and meaning of cryptography has been presented and how information security has become a challenging issue in the computer and communications sector. In addition to demonstrating cryptography as a way to ensure the identity, availability, integrity, authentication and confidentiality of users and their data, considering the important

aspects of protecting digital content and privacy, an algorithm has also been executed, through which data security and capacity has been increased.

Callas, J. [9] after his extensive study, cryptography has been described as a privacy-enhancing technique. He has mentioned the topics to be increased in the techniques of increasing the legal changes, credibility and privacy to maintain and operate the cryptography smoothly. He also explained what cryptographic technology is what society needs and what it will determine in the future for securing digital content. Here it has also been clarified that along with the general rules, existing laws and customs, what the society wants to achieve. These indicated that in which direction future researchers need to work more to fill the gaps of future to complete the process of cryptography. Furthermore, the future of cryptography depends on a management system that generates strong keys to ensure that only those with the appropriate keys can determine their access to the appropriate data. Callas also indicated that people's attitudes and views on security and communication privacy are mirrored by changes in the law.

By James L. Massey [10] Cryptography has two main goals: the first is authenticity and the second is confidentiality. In the context of data security, he has said that it can be either practical or theoretical. He discusses Shannon's principle of principled secrecy as well as Simon's principle of authenticity.

Lastly, Schneier [11] has concluded that the secrecy of security is a myth in order to accomplish a good task, because keeping security a secret cannot be considered good. Security can prove to be very fragile if it relies entirely on secrecy. Which will affects recovery after eating privacy, which will increase the chances of losing data. They have also clarified that cryptography based on small secret keys must rely on a fundamental principle that it can be easily transferred and changed. The cryptographic must be strong and public enough to provide good security. Emphasis has been laid on adopting public scrutiny as a way to further improve security.

Varol, N. et al. [12] presented an in-depth study on symmetric encryption, which can be used for encryption of a fixed text or speech. In this study, the content to be encrypted is first converted into an encapsulation chipper, which cannot be deciphered with the help of cipher algorithms.

Chachapara, K. et al. [13] also investigated and demonstrated the architecture using cryptography securely by cloud computing. This cryptography uses various algorithms such as RSA and AES. The AES algorithm has proven to be the most suitable for cryptography. Using cloud computing, different users can generate different keys with different permissions to access their files.

Gennaro, R. [15] presented ideas and discussions on the randomness of cryptography, trying to explain that a random process is one whose outcome is unknown. The unknown result led him to conclude that randomness is important in cryptography, as it provides a way to create information that cannot be easily learned by an adversary.

Preneel, B. [16] presented his views on cryptography and his approach to information security. Here he presented a comprehensive discussion and discussion on security practices and known methods for securing ICT systems. Under this, he also said that sophisticated attacking cryptography can be bypassed or weakened.

Sadkhan, S. B. [17] pointed out the main processes and trends in the fields of cryptography historically from the time of Julius Caesar to the present era. Along with this, he has mentioned the current conditions and circumstances of Arabic industrial and educational efforts. He has discovered new evaluation method for existing cryptographic and information security.

The basic concept of a cryptographic system is to cipher information or data in order to achieve confidentiality of the information in a way that an unauthorized person would be unable to derive its meaning. Two of the most common uses of cryptography would be using it to transmit data through an insecure channel, such as the internet, or ensuring that unauthorized people do not understand what they are looking at in a scenario in which they have accessed the information.

VI. Research Methodology:

Any research work is incomplete without research methodology. It is an essential task to use one or the other research method to complete the research work. The research methodology used in the present research work is as follows:

- Analytical Research Methodology
- Applied Research Methodology

Analytical research method has been used to analyse the traditional cryptographic techniques, with the help of which a comparative study has also been presented. Applied research methods have been used to enable the implemented cryptographic algorithms to be implemented. In between both the methods, quantitative and qualitative research methods have also been used. Qualitative research method has been used to perform and apply the quantitative and presented algorithms to conduct research work based on the quantity of different algorithms in the analysis of traditional algorithms. With whose help only success has been achieved in reaching a certain result.

VII. Conclusion:

Under the present chapter, it has been told that what the current scenario of cryptographic technology is. Techniques like cryptography have been described in detail and various literatures have been explored. Due to which it has become clear whether the research objectives of the present research work have been fulfilled or not. Special emphasis has been laid on the need and importance of cryptographic. Certainly it can be said that the present chapter has been successful in presenting the introduction of the entire research work. The research work has been completed on the basis of the proposed research methods. It is clear from here that what is the research problem and prediction of the presented research work. The present

chapter is fully capable of presenting the proposal of the entire research work, so that it can be clarified that the format of the direction and condition of the presented research work is correct and understandable.

VIII. Reference:

1. Aref, M. and Karim, F. (2017), 'Adaptive image steganography based on transform domain via genetic algorithm', Optik 145, 158–168.
2. Attaby, A. A., Ahmed, M. F. M. and Alsammak, A. K. (2017), 'Data hiding inside jpeg images with high resistance to steganalysis using a novel technique: Dct-m3', Ain Shams Engineering Journal.
3. Ayesha, S. and Masilamani, V. (2018), 'A novel digital watermarking scheme for data authentication and copyright protection in 5G networks', Computers and Electrical Engineering 72, 589–605.
4. Ayman, I. and Ibrahim, K. (2013), 'Wavelet-based [ecg] steganography for protecting patient confidential information in point-of-care systems', IEEE Transactions on Biomedical Engineering 60(12), 3322–3330.
5. Bakar, A., Othman, Z., Hamdan, A., Yusof, R. and Ismail, R. (2008), 'An agent based rough classifier for data mining', Eighth International Conference on Intelligent Systems Design and Applications 6, 145–151.
6. Biswas, K., Muthukkumarasamy, V. and Singh, K. (2015), 'An encryption scheme using chaotic map and genetic operations for wireless sensor networks', IEEE Sensors Journal 15(5), 2801–2809.
7. Blinowski, G., Januszewski, P., Stepniak, G. and Szczypiorski, K. (2018), 'LuxSteg: First practical implementation of steganography in VLC', IEEE Access 6, 74366– 74375.
8. Cao, J., Ma, M., Li, H., Fu, Y. and Liu, X. (2018), 'Eghr: Efficient group-based handover authentication protocols for mmtc in 5g wireless networks', Journal of Network and Computer Applications 102, 1–16.
9. Challal, Y., Ouadjaout, A., Lasla, N., Baga, M. and Hadjidj, A. (2011), 'Secure and efficient disjoint multipath construction for fault-tolerant routing in wireless sensor networks', Journal of Network and Computer Applications 34, 1380—-1397.
10. Chandra, S., Mandal, B., Alam, S. S. and Bhattacharyya, S. (2015), 'Content based double encryption algorithm using symmetric key cryptography', Procedia Computer Science 57, 1228–1234.