An AACO Based Optimized SWiFi Network To Reduce Overheads

[1]Gurleen Kaur, [2]Gurvinder Kaur
[1,2]GGS College of Modern Ttechnology, Kharar

***Abstract* - Nowadays the internet is Janus-faced with several challenges. Verifying data integrity and authentication are essential security services in order to secure data transmission process. Maintaining the security of your computer, network and private/sensitive data against unauthorized access and a wide variety of security threats without compromising the efficiency of the network can be challenging. The existing scheme enhance the data integrity, authentication and privacy depending on encryption/decryption methods by combining PGP, SWiFi and HMAC Systems in WiFi network but the efficiency of the system is reduced due to the overheads like delay, load etc. encountered during transmission. This research proposed a security technique to reduce the security risk across networks using PGP, sWiFi and HMAC systems with an efficient adaptive ant colony optimization (AACO) algorithm with uniform mutation operator using self-adaptive approach. Here mutation operator is used for enhancing the algorithm escape from local optima. The algorithm converges to the optimal final solution, by gathering the most effective sub-solutions where the probability of delay, load, retransmission attempts is very low and throughput is high. The proposed scheme gives better results than existing scheme as presented in results. The proposed technique is very complex for attackers to decode, and it is applicable to client-server architecture. The proposed system is expected to present, protect, and enhance the data integrity, authentication and privacy. Also, it improves the performance of the system. From the current study it may be concluded that the proposed system is more efficient than that of existing scheme.**

I. INTRODUCTION

A computer network or data network is a telecommunication network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the transmission media. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

II. WIFI ARCHITECTURE

The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement. When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block. A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

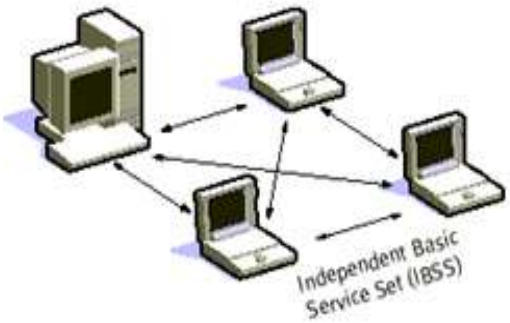

Figure 1 Wifi Adhoc Mode

When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS

becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points. Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, that is the Extended Service Set or ESS. The beauty of the ESS is that the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS′s transparently to the LLC.

III. AUTHENTICATION TECHNIQUES

Cryptography provides a straightforward approach for the transmitter and receiver to outline a set of valid messages that the transmitter will construct and therefore the receiver will verify [10]. Two kinds of cryptosystems square measure available:-

i) Personal key cryptosystems
ii) Public key cryptosystems

Private Key cryptosystems: Rhombohedral secret writing (also known as private-key secret writing or secret-key encryption) involves victimisation constant key for secret writing and cryptography. Secret writing involves applying Associate in Nursing operation (an algorithm) to the information to be encrypted victimisation the personal key to form them unintelligible. The slightest algorithmic program (such as Associate in Nursing exclusive OR) will create the system nearly tamper proof (there being therefore such issue as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Rhombohedral secret writing is based on the exchange of a secret (keys).

Public-key cryptosystems: Public-key cryptosystems also called uneven cryptography may be a category of cryptographic algorithms which needs two separate keys, one in every of that is secret (or private) and one in every of that is public. Though completely different, the two elements of this key combine are mathematically coupled. The general public key's wont to encrypt plaintext or to verify a digital signature; whereas the personal key's wont to decipher cipher text or to make a digital signature. The term "asymmetric‖ from the utilization of different keys to perform these opposite functions, each the inverse of the opposite – as contrasted with standard ("symmetric") cryptography that depends on constant key to perform each.

- Digital signatures: Digital signatures within which a message is signed with the sender's personal key and may be verified by anyone UN agency has access to the sender's public key. This verification proves that the sender had access to the personal key, and so is probably going to be the person associated with the general public key. This additionally ensures that the message has not been tampered with, as any manipulation of the message can lead to changes to the encoded message digest that otherwise remains unchanged between the sender and receiver.
- Hash Functions: A cryptologic hash perform is a hash perform that is taken into account much impossible to invert, that is, to recreate the input file from its hash price alone. These unidirectional hash functions have been known as "the workhorses of contemporary cryptography". The input file square measure typically known as the message, and therefore the hash value is usually known as the message digest or just the digest. The ideal cryptologic hash perform has four main properties:
    - it's simple to figure the hash price for any given message
    - it's impossible to come up with a message that incorporates a given hash
    - it's impossible to change a message while not changing the hash
    - it's impossible to search out two completely different messages with constant hash.

Cryptographic hash functions have several info security applications, notably in digital signatures, message authentication codes (MACs), and alternative kinds of authentication. They'll even be used as standard hash functions, to index knowledge in hash tables, for procedure, to notice duplicate knowledge or unambiguously establish files, and as checksums to notice accidental knowledge corruption. Indeed, in information security contexts, cryptologic hash values are generally known as (digital) fingerprints, checksums, or just hash values, although of these terms symbolize more general functions with rather completely different properties and purposes.

IV. RESEARCH GAPS

This approach can reduce the security risk across networks by combining PGP, SWIFI and HMAC systems. The proposed system is expected to present, protect, and enhance the data integrity, Authentication and privacy. Also, it increases the strength against network risks. Furthermore, our authentication system is very complex, which means that it is almost impossible to decrypt the method and also increases the transmission over heads.

V. DATA SECURITY AND PRIVACY PROTECTION ISSUES

The substance {knowledge|of knowledge|of information} security and privacy safety in cloud is analogous to standard data security and privacy protection. It is additionally concerned in each stage of the information life cycle. However due to directness and multi-tenant characteristic of the cloud computing, the substance of knowledge security and privacy protection in cloud has its particularities.

This means adopt by Organization for Economic Cooperation and Development (OECD) [5] is any info regarding associate known or distinctive individual information subject. Another accepted definition offer by the yankee Institute of Certified Public Accountants (AICPA) and therefore the Canadian Institute of leased Accountants (CICA) within the usually Accepted Privacy Principles (GAPP) standard is “The rights and obligations of people and organizations with relevance the cluster, use, and disclosure of individual information”.

Data Life Cycle

Data life cycle refers to the complete method from generation to destruction of the information. The information life cycle is divided into seven stages. See the figure below:

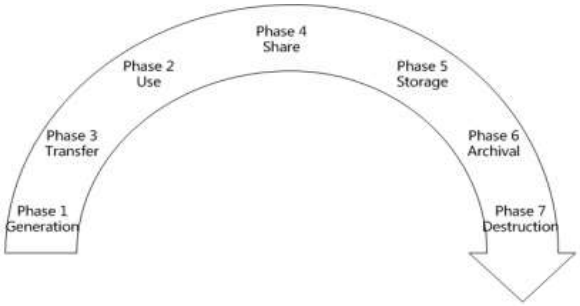

Figure 2: Data life cycle

A. information Generation

Data generation is concerned with the information possession within the ancient IT setting, sometimes users or organizations own and manage the info. However if information is to be migrated into cloud, it ought to be thought of that how to maintain the info possession. non-public} private data, information homeowners are entitled to grasp what personal data being collected, and in some cases, to prevent the gathering and use of private data.

B. Transfer

Within the venture boundaries, information broadcast sometimes doesn't need encoding, or simply have a simple encryption quantify. For information broadcast across enterprise borders, each information privacy and integrity ought to be ensured so as to forestall information from being broached and tampered with by unauthorized users. In alternative words, solely the info encoding isn't enough.

Data integrity is additionally required to be ensured. Thus it ought to make sure that transport protocols offer both confidentiality and integrity. Confidentiality and integrity of information transmission got to guarantee not solely between enterprise storage and cloud storage however additionally between totally different cloud storage services. In other words, privacy and integrity of the full transfer procedure of information ought to be ensured.

C. Use

For the static information employing a easy storage service, like Amazon S3, encryption is possible. However, for the static information utilized by cloud primarily based applications in PaaS or SaaS model, encryption in several cases isn't possible as a result of encryption can cause issues of compartmentalization and question, the static information used by Cloud-based applications is mostly not encrypted. Not solely in cloud, however additionally in typical IT environment, the info being treated is sort of not encrypted for any program to arrangement with. Due to the multi-tenant feature of cloud computing models, the info being processed by cloud- primarily based applications is stored in conjunction with the info of alternative users. Unencrypted information within the methodology may be a grave threat to information security.

Regarding the utilization of private information, things are a lot of problematical. The homeowners of personal information got to specialise in and guarantee whether or not the utilization of private data is consistent with the needs {of data|of data|of knowledge} assortment and whether or not personal information is being shared with third parties, for instance, cloud service suppliers.

D. Share

Data sharing is obtaining larger the utilization vary of {the information|the info|the information} and render data permissions extra complex. the info homeowners will allow the info admittance to at least one party, and successively the party will a lot of portion the data to a different party while not the consent of the info owner. Therefore, throughout information sharing, especially when information shared with 3rd party, the info owner need to think about whether or not the third party continues to take care of the initial protection measures and usage restrictions. Allotment of individual data, additionally to authorization of information, sharing coarseness all {the information|the info|the information} or partial information and data transformation are also got to be troubled regarding. The sharing coarseness depends on the sharing policy and therefore the division granularity of content. {The information|the info|the data} transformation refers to analytic sensitive information from the initial data. This procedure makes the info isn't relevant with the facts owner.

E. Storage

The data within the cloud could also be divided into:

(1) the info in IaaS setting, like Amazon's easy cupboard space Service;

(2) the info in PaaS or SaaS setting interconnected to cloud- primarily based applications.

The data hold on within the cloud storages is expounded with those hold on in alternative living-room and desires to mirror on 3 aspects of knowledge security: confidentiality, integrity and handiness. The acquainted clarification for information privacy is encryption. So as to make sure the effective of encoding, there must consider the utilization of along encoding algorithmic program and key strength because the cloud computing setting involving giant amounts of information communication, cupboard space and usage, there additionally must take into account processing speed and procedure potency of encrypting great amount of information.

In this case, for instance, regular encoding algorithmic program is a lot of appropriate than uneven encoding algorithm .one more key crisis regarding encryption is essential oversight. Is United Nations agency accountable for key management? Ideally, it's the facts owner aside from at here, as a result of the shoppers haven't adequate capability to supervise the keys, they often fork up the key administration to the cloud suppliers. Cloud providers got to carry on keys for an oversized variety of users; key

managing can become harder and difficult. Additionally to information privacy additionally must be anxious regarding information integrity. Once the users place many GB or a lot of information into the cloud storage, they the way to check the responsibleness of the data? As swift smoothness characteristic of cloud computing property, the users don't grasp wherever their information is being hold on. To move around out of or into the cloud storage can consume the user's network utilization (bandwidth) associated an amount of your time. Some cloud supplier like Amazon need users to pay transmit quantity the way to brazenly verify the integrity of information in cloud storage room while not having to initial transfer the info then transfer the info is a nice challenge. The info is active in cloud storage room, the normal technologies to ensure information integrity may not be effective. Within the ancient IT setting, the most threat of the info handiness comes from external attacks. Within the cloud, however, additionally to external attacks, there are many alternative areas which will threat the info availability:

(1) the provision of cloud computing services;
(2) whether or not the cloud suppliers would still operate within the future?
(3) whether or not the cloud storage services offer backup?

F. Archival

Archiving for information focuses on the storage media, whether or not to supply offsite storage and storage period. If the data is store on convenient media then the media is out of management, the info are probably to require the risk of outflow. If the cloud service supplier don't offer offsite archiving, the provision of the data are vulnerable. Again, whether or not storage period is in keeping with repository requirements? Otherwise, this may lead to the provision or privacy threats [15].

G. Destruction

When the info isn't any longer needed, whether or not it's been fully destroyed? Because of the physical characteristics of data-storage medium, the info deleted should still exist and may be improved. This could lead to inadvertently disclose of sensitive data [18].

VI. ACO

Ant colony optimization (ACO) is an algorithm based on the behavior of the real ants in finding the shortest path from a source to the food. It utilizes the behavior of the real ants while searching for the food. It has been observed that the ants deposit a certain amount of pheromone in its path while traveling from its nest to the food. Again, while returning to the nest, ants follow the same path marked by the pheromone and again deposit the pheromone on its path. In this way the ants following the shorter path are expected to return earlier and hence increase the amount of pheromone deposit in its path at a faster rate than the ants following a longer path. However, the pheromone is subjected to evaporation by a certain amount at a constant rate after a certain interval and therefore the paths visited by the ants frequently, are only kept as marked by the pheromone deposit, whereas the paths rarely visited by the ants are lost because of the lack of pheromone deposit on that path and as a result the new ants are intended to follow the frequently used paths only. Now, all the ants starting their journey can learn from the information left by the previously visitor ants and are guided to follow the shorter path directed by the pheromone deposit. In ACO, a number of artificial ants (which mimic the data packets) build solutions to the considered optimization problem and exchange information on the quality of these solutions via a communication scheme that is pheromone deposit on the path of the journey performed.

AACO: Adaptive Ant Colony Optimization (AACO) algorithm is a novel meta-heuristic algorithm that has been widely used for different combinational optimization problem and inspired by the foraging behavior of real ant colonies. Adaptive Ant Colony Optimization has strong robustness and easy to combine with other methods in optimization. In Self-Adaptive Approach, the parameters are encoded into pheromones and undergo mutation and recombination. The idea is that better parameters leads to better pheromones for finding shortest path or largest path, according to combinational problem. In [12], a self-adaptive approach, a single mutation rate is used. With this mutation rate p [0, 1], a new mutation rate p' [0, 1] is found using equation (1). In this equation, γ is the learning rate which controls the adaption speed.

$$p' = \left(1 + \frac{1-p}{p}\exp\left(-\gamma . N(0,1)\right)\right)^{-1} \qquad (1)$$

In this proposed method, Adaptive Ant colony optimization algorithm with uniform mutation operator using self-adaptive approach is used. Here mutation operator is used for enhancing the algorithm escape from local optima. In this method, an additional operator, mutation operator, is used and the new mutation rate is generated by the self-adaptive approach using equation (1). Here AACO algorithm generates the current solution (w). by using mutation operator, random position is changed by new mutation rate in current solution(w). After changing random position, new solution (w') is generated. Then the cost of this new solution (w') is compared by the current solution (w), if the cost of new solution is less than (or greater than) current solution, according to combinational problem, then new solution is replaced by current solution. This process is repeated until maximum iteration is not reached.

VII. PROPOSED RESEARCH

To overcome the drawbacks of existing technique Adaptive Ant Colony Optimization technique is used. Although the existing technique provides the security in swifi but it creates the transmission overheads in terms of delay, load, retransmission attempts, throughput and media access delay.

Description of transmission overheads are as follows:

- **Delay**: Delay of network specified how long it takes for a bit/packet of data to travel across the network from one node to another.
- **Load:** It refers to the amount of data that is carried by a network. It is expressed as bits/sec or packets/sec.
- **Throughput**: It is an average rate of successful message delivery over a network. It is measured in Bits/sec or packets/sec.

- **Data Dropped**: It is the amount of data that is not received to the destination and is dropped from the network. It is expressed in bits or packets.
- **Retransmission Attempts**: is the number of attempts that is taken by a source to deliver a message to the destination. It is represented in bits/sec.

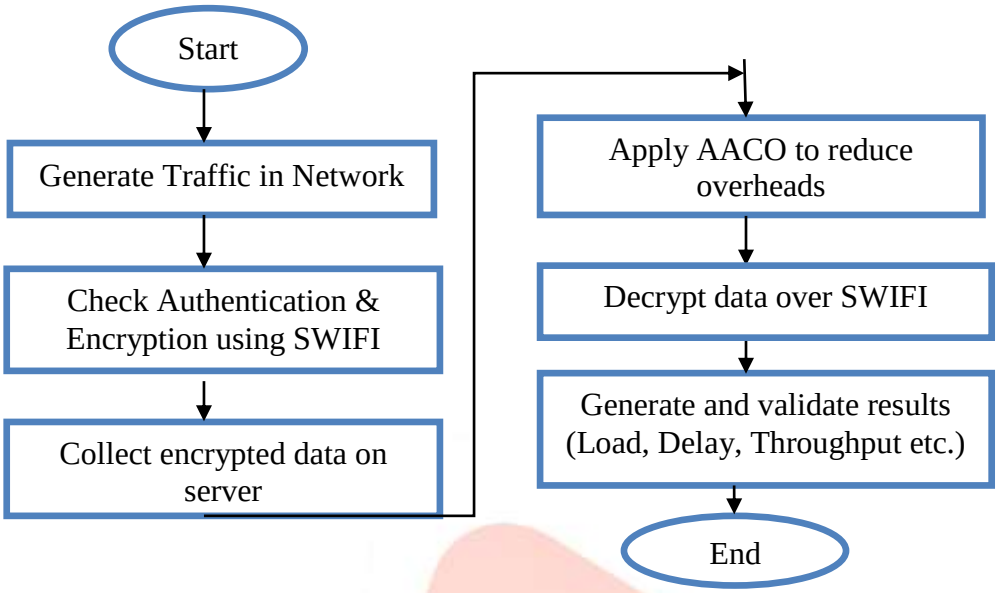

Figure 3: Flow Chart

VIII. Results and Discussion

OPNET is one of the most famous and popular commercial network simulators. OPNET Modeler is used to study and design communication networks, devices, protocols and applications. It provides a graphical editor interface to build models for various network entities from physical layer modular to application processes.

Delay: The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as: Avg. Delay=S/N, where *S* is the sum of the time spent to deliver packets for each destination, and *N* is the number of packets received by the all destination nodes.

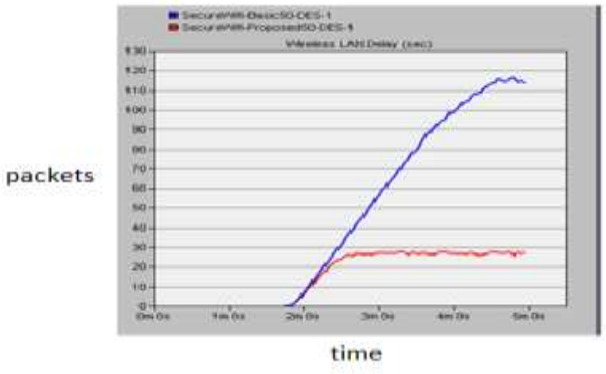

Figure 4: Delay

In the Figure 4 a comparative study for delay is presented. In the figure delay for existing scenario is approx 116 sec where as in proposed scenario it is below 30 sec.

Throughput: Throughput of a network can be measured using various tools available on different platforms. This page explains the theory behind what these tools set out to measure and the issues regarding these measurements. Users often concerned about measuring the maximum data throughput in bits per second of a communications link or network access.

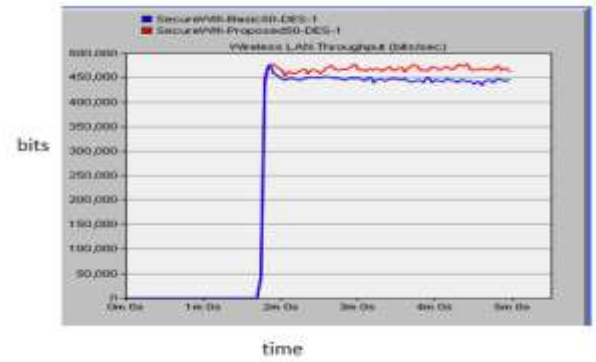

Figure 5: Throughput

In the Figure 5 a comparative study for throughput is presented. In the figure throughput for existing scenario is approx. 450,000 bits/sec where as in proposed scenario it is 475,000 bits/sec.

Retransmission Attempts: It is the number of attempts a source tried to send the packet to destination after being dropped in the network. It is measured in number of packets.

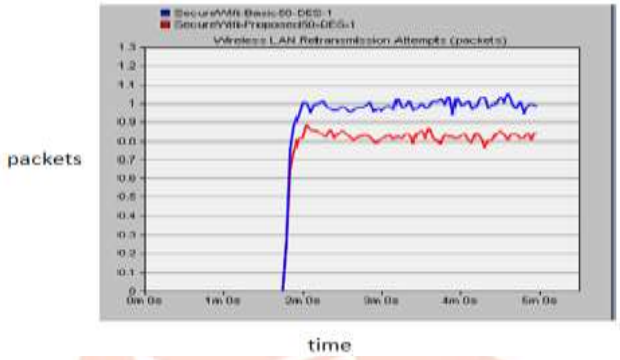

Figure 6: Retransmission Attempts

In the Figure 6 a comparative study for retransmission attempts is presented. In the figure retransmission attempts for existing scenario is approx. 1 packet where as in proposed scenario it is below 0.9 packets.

Load: It may be defined as the number of packets presented in a network at a time t.

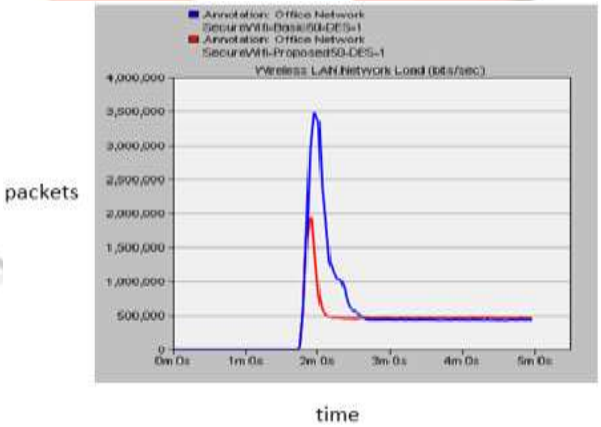

Figure 7: Network Load

In the Figure 7 a comparative study for network load is presented. In the figure network load for existing scenario is approx. 3,500,000 bits/sec where as in proposed scenario it is below 2,000,000 bits/sec.

Table 1: Comparative Study between Swifi and Swifi with AACO

Parameters	Secure Wifi	Secure wifi with AACO
Delay(sec)	116	30
Media Access Delay (sec)	116	30
Throughput (bits/sec)	450,000	475,000
Retransmission Attempts	1	0.9
Load (bits/sec)	3,500,000	2,000,000

Table 1 represents the comparative study of swifi and swifi with AACO. It shows the effective performance of proposed system in terms of parameters such as delay ,media access delay, throughput ,load etc.

- The delay probability in swifi is about 89% where as in the swifi with AACO system is about 23%.

- The throughput probability in swifi is about 90% where as in the swifi with AACO system is about 95%.
- The retransmission attempts probability in swifi is about 76% where as in the swifi with AACO system is about 69%.
- The load probability in swifi is about 87% where as in the swifi with AACO system is about 50%.

The percentage figures demonstrate that results of the proposed system are more optimal as compared to existing system.

IX. CONCLUSION

Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that use TLS are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The Internet of nowadays is Janus-faced with several challenges. One in every of the foremost discouraging challenges is to make sure security. Pursuing authentication through applicable mechanisms becomes a posh issue. Among different security problems, authentication and access control are the 2 main fields of security problems that should be resolved to shield info and computing systems against unauthorized access. In this research a scheme is developed using which security is implemented in authorization and authentication process. In spite of implementing the security in the secure Wifi the efficiency of the system is not reduces as presented in the results and discussion chapter. From the current study it may be concluded that the proposed system is more efficient than that of existing scheme. In the future scope proposed technique may be more scalable i.e. it may be applied to a large scale networks or on multiple access points. In this proposed technique encryption decryption overheads may be reduced.

X. REFERENCES

[1]. Ajeet Pandey, Alkhilesh Kumar Singh, "Ant Colony Optimization Based Routing Algorithm in Various Wireless Sensor Network- A survey", Journal of Advanced Computing and Communication Technologies, ISSN: 2347-2804, Volume No.3 Issue No. 4, August 2015.

[2]. Amandeep kaur, Shailja Kumari, "Secure Database Encryption in Web Applications", International Journal of Advanced Research in Computer and Communication Engineering,ISSN (Online): 2278-1021, ISSN (Print): 2319-5940, Vol. 3, Issue 7, July 2014.

[3]. Annapoorna Shetty, Shravya Shetty K, Krithika K, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", International Journal of Innovative Research in Computer, ISSN (Print): 2320-9798, Vol.2, Special Issue 5, October 2014.

[4]. Anubha Goyal, Geetanjali Babbar, "Lightweight Key Distribution for secure routing and secure information propagation – A Review", International Journal of Advanced Research in Computer Engineering & Technology, Vol: 4, Issue: 3, March 2015.

[5]. Alok Kumar Shukla, V. Kapoor, "Data Encryption and Decryption using Modified RSA Cryptography Based on Multiple Public Keys and 'n' Prime Number", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Vol. 3, Issue: 6, June 2014.

[6]. Bhanu Pratap Singh, Sohan Garg, "A Characteristic Study of Ant Colony Optimization Algorithms for Routing Problems", IJARCSSE, ISSN: 2277 128X, Vol. 3, Issue 3, March 2013.

[7]. Bonny B Raj, Panchami V, "DNA Based Cryptography Using Permutation and Random Key Generation Method", International Journal of Innovative Research in Science, Engineering and Technology, ISSN (Print): 2347-6710, Vol. 3, Special Issue 5, July 2014.

[8]. Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Mohsin Iftikha, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements", International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, May 2011.

[9]. Li Chen, Xingming Sun, Zhihua Xia, Qi Liu, "An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data", International Journal of Security and Its Applications, Vol. 8, No. 2, 2014, pp. 323-332.

[10]. Mupnesh Kumari, Priyanka Sharma, "Privacy Preserving using Homomorphic Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 4, Issue 7, July 2014.

[11]. Prabhat Kumar Singh, Gajendra Singh Chandel, "A Modified Technique For Performing Data Encryption & Data Decryption", ISSN: 2248-9622, Vol. 4, Issue 7 (Version 5), July 2014, pp.149-152.

[12]. Ramlakhan Singh Jadon, Unmukh Dutta, "Modified Ant Colony Optimization Algorithm with Uniform Mutation using Self-Adaptive Approach", International Journal of Computer Applications (0975-8887) Volume 74, No.13, July 2013.

[13]. Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol. 2, Issue 3, March 2014.

[14]. Ritu Pahal, Vikas kumar, "Efficient Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 7, July 2013.

[15]. Saranaya K, MOHANAPRIYA R, UDHAYAN J, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 3, March 2014

[16]. Shadi R. Masadeh, Ahmad Azzazi, Bassam A. Y. Alqaralleh, Ali Mousa. Al Sbou, "A NOVEL PARADIGM IN AUTHENTICATION SYSTEM USING SWIFI ENCRYPTION / DECRYPTION APPROACH", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[17]. Snehlata V. Gadge, "Analysis and Security based on Attribute based Encryption for data Sharing", International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359, Vol. 3, Issue-3, March 2014.

[18]. Srinivas B.L, Anish Shanbhag, Austin Solomon D'Souza, "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol.2, Special Issue 5, October 2014.
[19]. Sweety R. Lodha, S. Dhande, "Web Database Security Techniques", International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 3, March 2014.
[20]. T. Kiran, T.P. Anish, "Secure Hidden Routing in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 4, April 2015.
[21]. T. Sivasakthi, N Prabakaran, "Algorithm of User Authentication for Data Security in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol. 2, Issue 2, February 2014.
[22]. Vinh Hoa LA, Ana CAVALLI, "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY", International Journal on AdHoc Networking Systems (IJANS), Vol. 4, No. 2, April 2014.