journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

journal homepage: www.ojs.sabauni.net

Saba Journal Of Information Technology And Networking (SJITN)

Table of Contents

journal homepage:www.ojs.sabauni.net

Article

Survey of Privacy of User Identity in 5G: Challenges and Proposed Solutions

Mamoon M. Saeed[1*] , Rashid A. Saeed[2], Elsadig Saeid[1]

[1]*Alzaiem Alazhari University, Faculty of Engineering, Electrical Engineering Department, Sudan*

[2]*Sudan University, College of Engineering, School of Electronics Engineering, Sudan*

Article info

Article history:

Accepted: Mach. 2019

Keywords:

5G (Fifth Generation), Privacy, Identity, Paging, Location Tracking, IMSI (International Mobile Subscriber Identifier).

Abstract

This paper aims to shed light on survey about privacy of user identity in Fifth Generation (5G) networks and discuss various privacy issues of Fourth Generation (4G) with respect to 5G which use International Mobile Subscriber Identifier (IMSI) in clear text or join the temporary identities: Temporary Mobile Subscriber Identifier and Cell-Radio Network Temporary Identifier (TMSI & C-RNTI) with IMSI to disclose the privacy of user identity, after that the paper studies the proposed solutions to enhance the privacy of user identity and concludes that each of these studies have advantages and disadvantages for its proposed solutions. The fifth generation of mobile technology i.e. 5G is seen as a futuristic notion that would help in solving the issues that are pertaining in the previous generations. In fact, the key concern to many scholars in the field of mobile networking is user privacy, which is long-term subscription identifier as IMSI and short-term subscription identifier as TMSI and C-RNTI which use for permanent identifying, paging and location update.

* Corresponding author:
E-mail: mamoon530@gmail.com

1. Introduction

5G networks are the new generation in the life of upcoming cellular networks. It assures to present lower latency, further capacity and data rate. 5G has an amazing capacity for providing new amenities in order new usage circumstances of new activities, as an instance, in the smart homes, transport and healthcare. It increases their revenue, as well as it provides chances for industries and firms to construct new models in business to give uncommon amenities to people in extra enhanced and effective sorts. Different from the network with traditional cellular system, that are essentially designed for information transmission and speech [1], this revolution in different industry technological and different structure which vary in 5G, would carry a lot of defies for the privacy of user. The issues of privacy are the acute part to be considered in the explanation of 5G network as it is the most important to make balance in the services offered with respect to the privacy requirements of users [2,3].

5G networks will manage several applications and services which would presumably give new chances for a great amount of companies and activities which enable to interchange the information with huge data rate. This makes it clear that a big number from individual data would be approved over the 5G systems. The 5G networks should afford privacy contrivances in order to protect a diversity of important data, irrespective of persons as well as for engine-operators (e.g. location data, identity, movement decorations, subscribed services, system use manners, usually trustworthy usages, etc.) [4,5,6]. 5G system will likewise provide specialized system amenities to users via realizing the properties of specific amenities. Therefore the privacy requests in 5G networks, may differ from usage to other and from service to another. 5G system would furthermore support amenity-oriented privacy requests. For instance, a higher degree of privacy will be required to data related to health of the users in definite care of health usages. Furthermore, in the case of some serious manufacturing errands, there is strong need for advanced degree from protection of privacy. However, applications like penetrating for numerous compassionate of information of location might need a lesser level of privacy. For additional clarification, we have divided the privacy of user perceptions into three portions, which are; privacy of identity, privacy of location and privacy of data, see figure (1) [5,7].

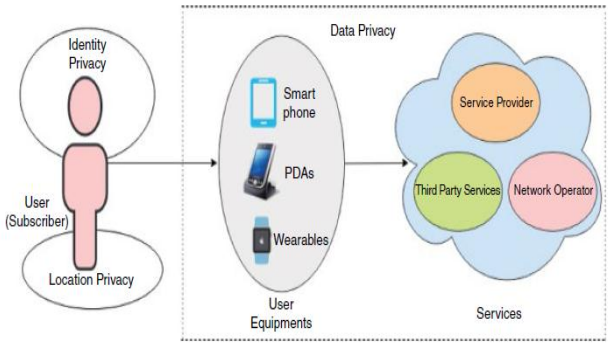

Figure 1. Various elements in user privacy.

The following privacy structures related to identity of user privacy are presented:

Location of user privacy: the attribute which the arrival or the attendance of a user in a definite region cannot be indomitable by overhearing on the coverage.

Identity of user privacy: the attribute that the long-term identity of user (IMSI) to whom an amenity is approved could not be snooped on the wireless entrance connection.

Intractability of user: the attribute which an interloper cannot presume whether diverse amenities are supplied to the similar user by overhearing on the coverage area [8].

2. Background

The 4G Long Term Evolution (LTE) standard requires Universal Subscriber Identity Module (USIM) on physical universal integrated circuit cards in order to gain network access. The high level of security and user openness must be an essential serving of 5G system, therefore the technique of handling identity will continue for achieving higher level of security. Entrenched Subscriber Identity Module (SIM) has also meaningfully dropped the tablet for placement issues associated to communication of machine-to-machine, there is a universal tendency of “bring-your-own-identity” [5], and the 5G network might commonly assist from an extra vulnerable identity organization design which permits for replacements. An instance could be to permit an inventiveness with a present, protected ID administration result to recycle it for 5G entrance. Exploratory different methods to handlebar subscriber or device identities is consequently a main contemplation that ought to go into the examination of the new belief replicas for networks of 5G. Conceptions such as system carving could offer an enabler for strongly permitting diverse ID organization answers face-by-face by restricting procedure to simulate, sequestered parts of the system [5, 9].

The Serving Network (SN), that could be organized by the operative, affords the definite mobility services and connectivity and the Home Network (HN) is organized by the operator where the user has a contribution.

The HN contains a Home Subscription Server (HSS), that clutches edges over that the SN could get authentication and other subscriber related information, and database of wholly operator's subscribers. The serving network authenticates the User Equipment (UE) before surrendering its service. Moreover, the SN validates a smart-card which includes USIM, which are put in the mobile equipment. The authentication is accomplished by the Core Network (CN) of the SN which is known by Mobile Management Entity (MME). The base station (called eNB) which is found in the Radio Access Network (RAN) that is linked to the CN to offer mobile access amenity. As of a commercial perception, the SN requirements guarantee which the mobile equipment retrieving the amenity could be justly indicted. The contribution validation process encounters this requirement by guaranteeing that the mobile equipment demanding entrance could be firmly connected with the data of validation which the SN has gotten from the HN for the mobile equipment [2,8,9,10,11].

The HN provider believes the SN provider to validate the mobile equipment by data of validation which the HN offers. Annotation that the HN provider does not believe the SN provider by the definite permanent qualification for authentication.

As an alternative the HN assures that the SN provider by previous data of validation practical is used for authentication and creation of session key. The HN provider moreover proclaims the SN provider in order to deliver right accusing data linked by the amenities recycled through the mobile equipment rendering to the wandering arrangements among the twofold providers. The SN provider makes definite that the home subscription server in the HN offers data of validation which could validate a distinguishing mobile equipment accompanying with that HSS [12]. LTE uses a three-party protocol which are HSS, MME and eNB (as shown in figure (2)) in order to session key creation and contribution validation, which is called "Authentication and Key Agreement (AKA)" [11].

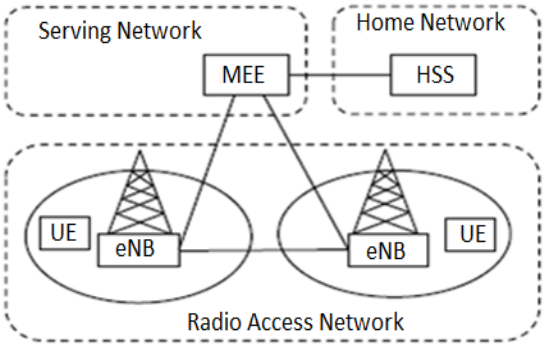

Figure 2: General architecture of a basic 4G network [18].

Symmetric key K is the foundation of authentication and key agreement and the conforming international mobile subscriber identity (IMSI) mutual by the HSS and the smart-card. Whereas systems of 3GPP usage dual diverse varieties of authentication and key agreement, the first one is created through second generation and the final was presented through third generation, in this survey we would contemplate only with the latter. Third generation offers shared validation and it is the merely permitted type in fourth generation, while Universal Mobile Telecommunications System (UMTS) and Global System for Mobile communications (GSM) permit both types of authentication and key agreement. The three festivities complicated in authentication and key agreement are the USIM card inserted in the mobile equipment, the mobile management entity, and the home subscription server. Upon fruitful accomplishment of authentication and key agreement, the mobile management entity contemplates the smart-card valid. Subliminally, the mobile management entity at that time moreover contemplates the intact mobile equipment and the user valid.

Formerly authentication and key agreement is originated, the mobile equipment delivers the international mobile subscriber identity to the mobile management entity. On the other hand, if the mobile equipment has been allocated a temporary mobile subscriber identity, which recycled as a replacement for the permanent identity. The mobile management entity determinations the temporary identity with the conforming permanent identity in this case (see figure (3)).

As soon as the mobile management entity gets the permanent identity, it demands authentic data between the HN and the HSS. This data of authentication is refunded in the procedure of a content (XRES, KASME, AUTN and RAND) by the HSS, where XRES is the predictable

answer to the test, KASME is the key of session conforming to the test, AUTN is an authentication token of network, and RAND is a challenge for the User Equipment (UE), this procedure is mentioned by an Authentication Vector (AV). Mobile management entity onwards the AUTN and RAND to the user equipment, and the UE onwards the AUTN and RAND to the smart card. The smart card authenticates if the AUTN is right and renewed. If the confirmation bombs, the smart card discards the validation. Then, the smart card analyzes the key of session KASME and creates it obtainable to the user equipment composed using the RAND in order to the answer RES. The RES directed back by the user equipment to the mobile management entity, that could make comparing between it to the predictable answer XRES which gets it from the received data of validation by the home subscription server. In this study we would ignore the authentication protocol the details which are not correlated to the characteristics of privacy to the international mobile subscriber identity [8,10,13].

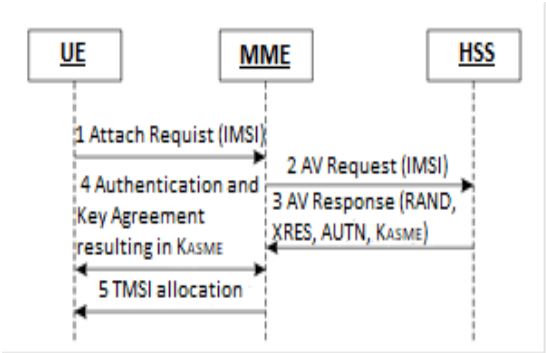

Figure 3: A basic sequence chart of communication for Authentication and Key Agreement (AKA) [18].

The risk of "IMSI catching", wherever scoundrel wireless system paraphernalia needs movable equipment in order to disclose the user identity, which was discoursed throughout the UMTS and LTE systems enlargement. Nevertheless, at that time there is no presence of any defense appliance, as the expectable extortions did not appear to defend the complexity or cost complicated. It is not vibrant whether this analysis of danger is tranquil lawful, or improved protection of international mobile subscriber identity justifies contemplation for 5G networks. A number of mechanisms are adopted by mobile networks to overcome security vulnerabilities which improve the privacy of the 3G and 4G [8,14,15,16].

3. User privacy issues in 5G

The experience of the IMSI is the focal issue of privacy in the 3GPP is. The international mobile subscriber identity could be interrupted through oppositions. Like outbreaks are usually denoted to as "IMSI catching" [5]. The 3GPP assigns numerous diverse provisional identities like C-RNTI, M-TMSI, and Global User Temporary Identifier (GUTI) for a single mobile equipment within 3GPP system construction for diverse interacting amenities to defend the privacy of user identity. The mobile equipment in order to identity itself to the network to start amenity requirements, it could make use of those identities as an alternative of the permanent identity.

The user identity is remained defenseless to assaults of privacy despite of security organization. There are some actions, which the mobile equipment wants to identify itself with its international mobile

subscriber identity (in unblemished version) [15]. Such instances: (1) Whenever the mobile equipment attaches to a different SN which bombs to get the information of user equipment from the last SN; (2) Through the first assign connection; (3) When the SN could not recover the temporary identity of the mobile equipment. Also, it is not enough to stop IMSI disclosure when it uses of provisional identifiers like GUTIs. GUTIs keep on officially for long period and re-used by diverse areas and could be recycled by inactive assaults to obtain permanent identity [8].

In order to provide a further level of security to guarantee related validation lengthways by preserving the openness of user and privacy, the management machine for the identity in a 5G network would be a critical career. As it is known 5G network required to defend the network and the identity from unsanctioned entrance of users, it would also develop a high many-seller situation and include numerous shareholders and a robust identity machine of administration. Throughout the normalization procedure of UMTS and LTE, once paraphernalia like portable equipment's display their definite individualities, there is a thoughtful risk concerning permanent identity catching. On this time, there is no machine to protect user identity suggested, for the reason that specific risk has not produced any thoughtful distress to the entree system. It is not totally crystal clear yet that if this assailant is remain lawful for 5G system and requests several additional contemplation [7].

A present study to protect identity of subscriber is built on a SN allocating a arbitrarily created provisional identity such as TMSI for the user equipment at steady interims. The permanent identity IMSI is recycled merely as a responsibility retrieval machine and when a temporary identity has not yet been allocated. The retrieval machine is required to evade lock-out of a user equipment once mistakes happen, an example, when the mobile device or SN has misplaced the temporary identity.

When the SN needs to use permanent identity, the user equipment returns back to use the international mobile subscriber identity, in this retrieval machine the IMSI-catchers adventure could get the permanent identity from the user equipment. Therefore, the present method of keeping user privacy does not offer any defense in contrast to an vigorous assailant on the radio link, demanding to be a authentic system that has missing the TMSI. Addition to that there is no any defense in contrast to inactive observers who are existing as soon as international mobile subscriber identity requirements are accomplished [8,16,17,18].

A. Identity management

International mobile subscriber identity catching assaults could be either inactive or vigorous, or both of them. In inactive assaults, if it snoops in the region of the radio coverage, the permanent identity could be collected and captured by the identity attacker. However, in case of vigorous assaults, as we know the user equipments commonly choose the eNB with the maximum power of signal and imitation eNB which is recognized to get

robust power of signal and could be deliberated like a real eNB. Then it send a communication demanding the identity to overall user equipments which are in the exact region by this imitate eNB. user equipments transmit their permanent identity to imitation eNB as legal eNB for UEs, that have missing the joining to temporary identity. GSM identity catching is often hypothetical to be an initial purpose for extra comprehensive snooping occurrences. There is improvement method which is stated in [19], that permits operators of HN to put their belief fewer on SNs and protector in contradiction of permanent identity catchers. The HN and the user equipment could get the permanent identity in clear version, therefor the idea is to improve the management of protocols and identifiers [18].

Because they are doing as a legal system which has gone astray momentary identity and whenever the demand for permanent identity is completed, here is no suitable defense for inactive observers which probably could be offered there, the standard privacy protective machines do not have assure defense beside the dangers on radio coverage [19]. Numerous confidentiality linked assaults have been described, for example in some circumstances when a imitation eNB is planned foremost to the beginning for individual data of mobile user. Essentially permanent identity assaults are dedicated on thieving international mobile subscriber identity of a user equipment .The temporary identity catcher demands from the user device the identity of user in place of the extended period. This is deliberated as a usual unchanging demand and answer, user equipment transmits its permanent identity by typical technologies of security. From this time the catchers of permanent identity are used to display and pathway the definite users locations.

5G networks, equipments and devices such as smart sensors, smart devices, and wearable devices would be moderately slighter in size and too reasonable to billet smart card like the customary wireless networks are commonly reliant on smart card (USIM) cards, in order to accomplish keys and users identities. So, to handle the device identities, the unusual approaches are requested in this event [12,20]. There is probability of a background which could be include the service identities and device collected.

Through the industrial stage, the identity of mobile could be assigned and is deliberated as an inimitable universal identity. By a way, of examination supplier presents the identities of amenity. Identity of equipment is also mentioned to as the smart card identity could identify one or several identities of amenity. It permits mobiles to create their assessment apropos that specific mobile could be allowed to enter the system and develop the given amenities [20,21].

The network of 5G might require further malleable and exposed administration substructure for identity, that must have the opportunity to several substitutions and be capable to offer agreement for that. To make this happens for businesses, they may permit the current mechanism of identity administration to use again for 5G entree. By 5G network, there could be a huge amount of hand-detained equipment

which might contain tablets and smart devices, as well as wearable's; so it is significant to discover methods on how to keep the identities of users and at the same time how to hold those equipment's. For 5G systems it is also critical to consider unusual reliance prototypes. A number of important concepts need to be mentioned here such as slicing and virtualization system, that need to deliberate when suggesting the protected methods of user privacy [22].

B. User identity privacy issues

Mobile users do not need to disclose their unique personality to service providers or to other users when the users obtaining services on definite instances. For instance, the user desire to stay unknown when requesting online any questions or sending response of establishments. In a number of circumstances, subscribers could use momentary or identities incorrect and reject them once the requisite job is accomplished. Awareness of perpetual identity of a subscriber might authorize an enemy to pathway and collect complete information around personalities. These days, the tendency of thieving website personalities is further communal. There are several websites applications such as banking and shopping which could need credit cards to payment online. By these profiles, the adversary can lead to illuminating the actual personality and could source probable threats to the privacy of user. Commonly, several methods tray to confide the actual identity [10].

I. Permanent user identity issues

The central privacy problem within the 5G system and previous generations is the disclosure of the international mobile subscriber identity; the permanent identity could be interrupted by challengers (active or inactive assailants), such spasms are usually referred to as "catching of IMSI". The assailant can path the appointments of the mobile device and at that time disrespectful the privacy of users. The 3GPP assigns numerous diverse provisional identities such as C-RNTI, GUTI, and M-TMSI to a particular mobile user at diverse stages of 4G system construction, to defend the privacy of user identity [23].

The mobile equipment could apply those temporary identities in its place of the permanent identity to characterize itself to the SN to start amenity demands.

The user equipment in some circumstances used the permanent identity (IMSI) and send it in clear text when the mobile equipment is demanded to identify itself to the SN. There is a number of instances such as:

- Where the SN (mobile management entity) could not recover the GUTI of the user equipment .
- During the first attach process.
- The IMSI may be exposed by the user equipment when the user equipment replies to an imitation verification demand originated by a choice eNB which is personating a unaffected eNB.
- When the user equipment hand off to a new mobile management entity, which bomb to obtain the permanent identity of the user equipment from

the last mobile management entity.

As a result of information of the permanent identity to serving network; this might denote additional risk to the user privacy [8].

II. Paging procedure issues

The paging procedure used in the network to find the mobile user for purpose carry an amenity for it (e.g. SMS message, an arriving connect). Here are diverse cases for the UE as idle and active form. MME detects the UE in idle mode as per following area basis. The MME sends the paging demand message to all base stations within a specific following region. The message of paging is transmitted on a broadcast channel and the identity of one or more mobile users is hold. The mobile users anticipated by the request of paging which typically recognized by provisional identities (TMSIs) to offer obscurity of the user equipments [4,16,24].

The mobile user creates a devoted radio channel to permit the transfer of the sequential replying to incoming the SMS or delivery call when it catches its temporary identity in the message of paging, it. It must be illustrated that temporary identity would not be different inside a definite Area of Tracking (AT) and the message of paging are not scrambled.

When the UE and SN start a paging demand for a definite temporary identity, it permits an assailant to discover the attendance of a specific user equipment inside a definite region. Suppose that an assailant starts a communication to a definite UE inside tracking area of users. At that time, the assailant observes the radio channel of paging to get a group of temporary Identities which have been called by the base station.

When reiterating the assailant frequent intervals and finding numerous groups of temporary identities, the assailant might disclose the temporary identity of the envisioned usages by interconnecting the groups of temporary identities (TMSIs) as shown in figure (4). The issues of privacy in paging process might threat the location privacy addition to intimidate the privacy of user [4,5,16,24].

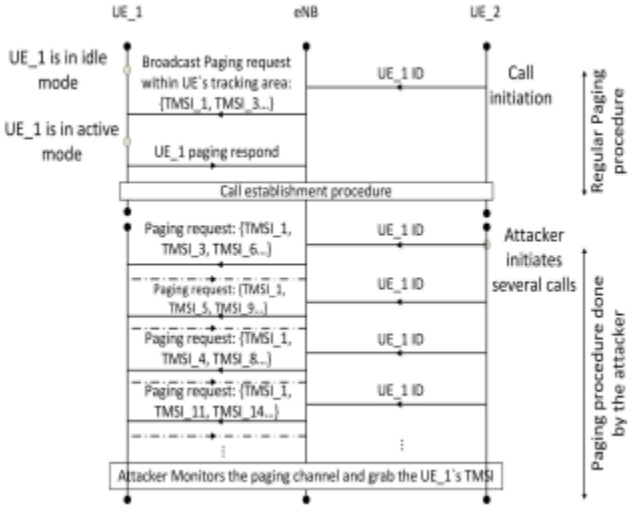

Figure 4: Paging procedure and the respective attack.

III. Location privacy issues

The other risk to the user privacy in 4G and 5G is Location Tracking (LT). LT denotes to the probability of following the arrangements of a definite user by a third party [25].

The eNB allocates diverse provisional identities Cell-Radio Network Temporary Identities (C-RNTI) to a user equipment throughout the transferring within the eNB's coverage from one cell to another, to confirm untraceability of users and to escape LT. Although, the UE uses

different C-RNTIs accomplishment, however the location tracking remain probable. The C-RNTIs allocated to user equipment that might be related, may be followed by an assailant. Even if the attacker was inactive to the location tracking, he may convert more evident, who is observing the wireless channel from the instant the user equipment started an assailant process, might join the different C-RNTI allocated to the user equipment by the base station with the IMSI. The assailant could register the positions stayed by the aim that subscriber saves a subscriber outline previous region as shown in figure (5). Location tracking characterizes a thoughtful intimidation to the privacy of user which must not be disregarded [5,16,23].

=

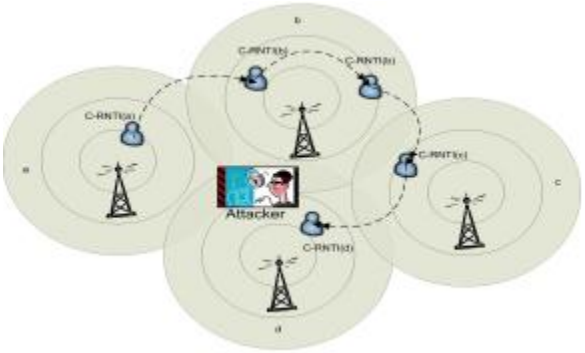

Figure 5: Location tracking attack using C-RNTI.

There are little obtainable methods existing for protecting the privacy of location which could moreover be suitable in the situation of privacy of location defense in 5G networks. Public procedures recycled to defend the privacy of location of the customer might contain penname difference, anonymization and track disconcertion [10]. Supervisory methods are moreover wanted, consequently that robust rules, principles and legislature could be intended for suitable use of the system, placing the consciousness above of the description of system and internet confidence [11].

Encryption procedures are amongst more obtainable methods to defend the consumers location confidentiality. Permanent identity catching is carefully associated to the subject of confidentiality of location. Deliberate international mobile subscriber identity of UE permits the invader to pathway the appointments of user and generate outline around the UE and therefore ruptures the location privacy of user [26]. Likewise, attacking privacy of location bullies identity privacy of user. Permanent identities might be gathered at particular locations similar to workshop facades, wherever the workshop custodians gather permanent identities over waveforms of Wi-Fi for the perseverance of appraising the efficiency of their workshop facades [27]. Furthermore, LBS that has the aptitude to pinpoint a user equipment geologically could bullies the user's privacy [5,24]. The gathered permanent identities of a specific UE at a particular region might be recycled to attack privacy of users and observe the UEs at different regions as definite by the aggressor to accomplish risky assaults in contrast to it [13].

4. Proposed solutions and discussion

Contribution of a user privacy has been a chronological anxiety through every preceding generation portable systems, specifically, LTE, UMTS, and GSM.

However, a slight development has been accomplished in obtaining the privacy of the long-term identity of a user, paging procedure and location tracking, so the IMSI catchers are tranquil in presence even in the advanced LTE and LTE systems. Suggestions have been available to challenge this difficult in 5G networks built on pseudonyms and various public-key machineries.

To sanctuary the user privacy in 5G systems, there are a lot of papers which discuss this issue and propose solutions, the researchers have gathered some proposed to this problem that can be furnished in the following section.

A- Proposed solutions for permanent user identity

Through the initial stages of 3G, 4G and 5G networks, some improved permanent identity protection machineries were discoursed. Three choices are there: (1) encrypting IMSI using private key, a public key of the serving network or using a mutual group key, (2) using pseudonyms to hide IMSI, (3) proposing new format to change AKA and hide IMSI.

1- Studies used encrypting IMSI

There is a great number of studies which used a shared group keys, a public key of the serving network or private key to hide IMSI in 5G, of those are, there are researchers looked into the challenging of obscuring long-standing identity of a user and offer a method built on identity based encryption to challenge it. They discovered that the suggested solution can be comprehensive to a key agreement protocol and shared validation between a mobile user and a SN. This shared validation and key agreement procedure does not require to connect by the HN on each run. And they made a qualitative evaluation for the benefits and weaknesses of diverse methods that display that their way out is good for protecting the permanent identity of a UE in the 5G system.

They presented a protocol that works on the determinations of both secrecy endangered identification of user equipment and shared validation between user equipment and serving network. This shared validation does not need a communication with the home network every interval the procedure is run between a serving network and a user equipment. Their answer is that they did not make use of PVT, however, in its place usage an expiration period by pre-agreed design. This expiration period can performance by way of the PVT. If the public key of an identity requests to be canceled, the expiration period lengthways using the identity is additional to the cancellation tilt. If the identity needs a different public key, the PKG usages a different expiration period to calculate the private key of the identity. The recently calculated private key is at that time provisioned to the identity lengthways with the different expiration period. Once the expiration period derives, completely the public keys calculated by the expiration period are mechanically canceled. Thus, the cancelation menu does not require to contain cancellations whose expiration period is in the previous [28].

In a similar manner, in another paper by the same researchers, they examined long-

standing individuality of a subscriber and offered a procedure built on identity based encryption to challenge it. They suggested an answer that can be prolonged to a shared AKA between a mobile user and SN. However they named the procedure Privacy Enhanced Fast Mutual Authentication (PEFMA). The serving network does not requisite to join on user equipment by the HN and the serving network has public keys. A user equipment directs the permanent identity once encrypting it by the public key of serving network. As the serving network and user equipment have public keys, privacy enhanced fast mutual authentication can run deprived of communicating the home network. Hence a fast mutual authentication is realized when SN and HN are placed far from each other.

They came to the conclusion that a procedure which helps the determinations of both shared validation between serving network and user equipment and privacy protected identification of user equipment. In PEFMA, the HN is the PKG. PEFMA does not apply PVT, however, in its place usage an expiration period, this expiration period could perform equally to the PVT. HN calculates private keys of all of its users using their IMSIs and appropriately selected ETs.

These private keys are provisioned to the UEs using a secured channel. The serving networks which have a peripatetic bargains with the home network are moreover provisioned with their particular private keys by the home network. Before the expiration of the expiry time, a UE or an SN may demand for a new private key to the HN. The HN would choose a new ET, compute the private key and send the new private key to the UE or to the SN in a secure channel. A UE may request for a new private key if the UE considers that the private key has been cooperated [29].

On the other hand, there are some researchers presented the developed Mobility Support System by MEC as a key primary to defend a portable users system secrecy with slight influence on communication enactment. Their solution is that though the scheme process price is abridged more, mobility support system might too nearby the fissure of joining intermission for wandering portable consumers. They offered improved (mobility support system) scheme with MEC, by leveraging cellular system's omnipresent system properties comparing to characteristic VPN and cellular system, mobility support system with MEC could offer an improved system privacy defense, at an reasonable functioning cost with a little extra added remunerations [30]. Similar this study, there are other researchers evaluated an Android execution of one of the improvements, which contains the unequal method Elliptic Curve Integrated Encryption Scheme (ECIES). They concluded that it is possible to instrument unequal encryption approaches for the continuing contribution identifier and that the underscored secrecy faintness can be professionally disputed. This eliminates one more set of difficulties for recognizing the defense in portable system principles. Furthermore, they offered the effect of their applied estimation of encrypting the IMSI in 5G networks by using elliptic curve integrated encryption scheme (without MAC). They

used two crypto libraries, Nettle and Open SSL, and made the test for the enactment in four Android-based strategies [31].

In the contrary other researchers presented structures for 3GPP AKA which offers faultless onward privacy for the session key. The concepts avoid an assailant, through entrance to the long-term pre-shared key, from merely snooping the test RAND in the authentication and key agreement route, and usage the RAND and permanent pre-shared key to descend the session key. They dedicated on creating it conceivable to re-use great slices of the present construction of 3GPP occupations and interfaces, with the basis that this will create the structures further expected to be approved by the industry. In particular, the structures keep up the line in the middle of the mobile equipment whole and the USIM card . By way of a significance, there is no necessity to roll out different identifications to obtainable consumers.

They found that it is applicable to extant PFS and defense in contradiction of inactive assaults on the communications link security keys into the current construction and procedure constructions mutual by preceding generations of 3GPP systems. The structures do not affect the USIM card and mobile device interface, and consequently permits re-use of the current organized universal subscriber identity modules although extortions motionless continue to the sitting key K'ASME. They come to conclusion that it is conceivable to bound the belongings of a settlement of K (even if it occurs previously at industrial period), and that achievement is conceivable with reasonably slight influence on the legacy 3GPP constructions. Nevertheless, due to rearward compatibility subjects, it is perhaps not essentially probable to present this in traditional networks, but it is slightly functionality for 5G networks [32].

Another study concerning to encrypt IMSI had been conducted other researchers, where the main aim was to protect identity privacy of a user in 5G by hiding the identifier of the consumer. In order to direction the hidden identifier to the suitable target, definite data approximately the IMSI – NC and CC, must be publicized. However, as was lately barbed, the routing requirements for validation data between home network and visited network, and also requests other data around the international mobile subscriber identity to be publicized within the home network. As it was mentioned that there are boundaries on user identity privacy outstanding to official interruption in the SN. In this fresh perspective, the authors reconsider distributed different answers of privacy of identity. They found that the up to that time favorable answers example, answer based on public key of HN turn out to be fewer hopeful. And they found that the way out built on identity based encryption converts extra favorable than it was previously [33].

The researchers proved that these solutions have used several encryption approaches by using public key or private key cryptography to encrypt the identity as shown in figure (6). Although the encryption offers obscurity of the user, the extraordinary calculation involvedness and message above by way of a product of communicating encrypted identity. This may add new components and overhead in

expressions of both bandwidth and calculation period.

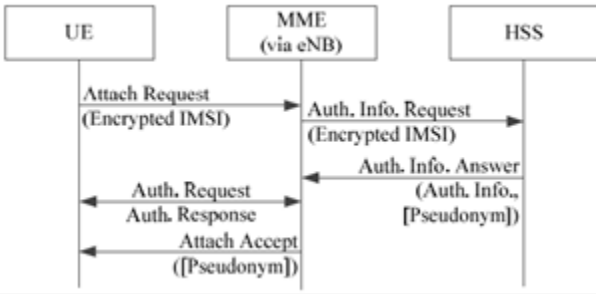

Figure 6: Simplified attach procedure using encrypted IMSI [33].

2- Studies used pseudonyms to hide IMSI

There is a number of studies which used pseudonyms to hide IMSI in 5G; those are researchers presented a novel scheme for defending the international mobile subscriber identity by incomes of creating a pseudonym between the HN and the UE. The pseudonym is derivative locally at the HN and the UE without an acting obtainable USIMs. They analyzed the explanation from a methodical perception, as well as from a monitoring and functioning perspective. They said that the obtainable technique defends the international mobile subscriber identity from active and inactive permanent identity catchers as well as truthful but inquisitive helping systems. Furthermore, it can recuperate from lock-out conditions where one party has misplaced the penname.

In their conclusion, they claimed that there are two main stages. First, they defined a first attach by the user equipment when it does not join any penname with the SN nor with the HN. The outcome of this stage is that the user equipment is allocated a pseudonym P by the HN and a temporary identity (TMSI) by the serving network. Next, they defined the second stage where the user equipment no lengthier stakes a temporary identity with the SN and it is enforced to detect itself using P when P has been used, it is changed by a fresh penname to confirm unlink ability [27].

Other researchers thoughtful study, detailed the user traceability risk acknowledged in LTE-WLAN Interworking (LWI) and proposed new concepts to moderate the acknowledged risk by use of 3GPP system locally administrated randomized address for the user equipments WLAN MAC address as a replacement for generally managed MAC address. The locally administrated randomized address is created using the 3GPP system allocated pennames, so that the users privacy (device identity and disappear effective and secure as the 3GPP networks. Amongst the comprehensive original concepts, the locally administrated Randomized Address created by means of the essential network allocated pennames discourses the users privacy efficiently and has fewer than 1% pileup possibility.

They found that uniform in 5G networks it is not probable to hide the international mobile subscriber identity continuously. But, there are contrivances to reduce the risk using brief identities. But in the 3WI situation, with smallest energies, it is possible to pathway a user and pedestal user exact besieged assaults in the 3GPP RAT using the WLAN MAC address compare to the international mobile subscriber identity established following. Consequently, to accomplish the present level of protection in the 3GPP system,

WLAN MAC address should be obscured [34].

The researchers found out that these ways specifically attempted to improve pseudonym in 5G. Nevertheless, the methods have various deficiencies: On one hand, it is comparatively difficult, with numerous novel cryptographic utilities. The administration of pseudonyms would requisite superfluous handling exertion and memory cost. On the other hand, the distribution of pseudonym to each user equipment from the network inhabits extra bandwidth. In adding, the quantity of computational exertion for mobile devices is extraordinary since IMSI is exchanging with each authentication process. This increases convolution in various of the utmost essential and repeatedly performed processes in network.

3- Studies proposed new format to change AKA to hide IMSI

There is a considerable number of studies which proposed new format and architecture in 5G network. Those are researchers elevated the issues related to Wi-max and LTE which were deliberated at physical and MAC layer level. They also explained the revolutionary 5G architectural framework and how 5G technology would integrate a more secure environment for hand held devices. They suggested to improve security in 5G by creating it flexible architecture of 5G networks which permits reliance models to be built. And it also analyzed five supports of power of 5G network security which can effort in cooperation with each other to afford the users with a secure mobile computing environment [35].

Other researchers suggested a new scheme typical for a 5G network allowed vehicular system that enables a and privacy-aware and protected video recording amenity. The eventual impartial of this amenity is to immediately bang the videos of transportation accidents to the adjacent authorized vehicle in order to develop protection on the streets. They suggested reportage amenity procedure is considered to profit benefit of the estimated structures of 5G systems in statuses of low latency, great-speediness contacts, and abridged price. Furthermore, it offers robust privacy and security in contradiction of assaults that try to pathway a partaking vehicles identity or disclose the subjects of the described accident audiovisual. The privacy of the partakers is sheltered in contradiction of interior and exterior challengers that force settlement slight cells, communications of device to device pass on or the cloud stage. Also, the suggested procedure assures that inadequate despoiled establishments cannot disclose the identity of a contributing vehicle and collaboration amongst an ratified numeral of diverse specialists have to take place to do that, and analyzed the effectiveness of the suggested amenity and presented that a transportation coincidence video can be detailed in a protecting and privacy-conserving method in fewer than one minute to the authorized vehicles to assurance a rapid reply in the direction of transportation coincidences [36].

On the other hand, there are other researchers presented a prospective communication of D2D construction that is assimilated into the LTE networks. In the

LTE Evolved Packet Core (EPC), a ProSe purpose and ProSe app server are presented to knob the communication of device to device process and to offer proximity-based application amenities for D2D operators. To eliminate the system connection, the ProSe utility component is software defined in the LTE-EPC. The ProSe utility interrelates with the MME and the HSS, and collaborates with the ProSe app server on several features counting the packing of user-specific arrangements, the administration of the ProSe amenity recording, privacy protection, authorization, security, annulment and device detection and so on. They discovered that the ProSe server can use the site data from mobile management entity to identify the nearness between user equipments and explosion probable communication of D2D occasions to the application server. The HSS has an association with the authentication center, and holders authentication requirements from the mobile management entity. In the in-coverage situations, the sitting is primed from user equipments to mobile management entity, and reciprocal validation is conceded out. The serving gateway is accountable for the user equipments environment administration and storing, movement switch, and paging activate. The Packet Data Network (PDN) gateway offers the connectivity and data raise from the Internet or outside system for the user equipments [37]. Similar to this study, there are further researchers proposed two Key Agreement protocols and Privacy-Preserving Authentication (PPAKA-IBS and PPAKA-HAMC) to assure protected and unknown Device to Device group communications. However their difference lies on their protocols, a set of device to device users reciprocally validate with each other deprived of seeping their individuality indication while exchange a public device to device set session key for protected infrastructures in a device to device session. Official security enquiry and complete presentation estimation display affectivity and security and their protocols.

They found out that the first protocol PPAKA-IBS can establish secure device to device set communications by given that better security than PPAKA-HMAC in positions of attacking interior assaults. The second protocol PPAKA-HMAC aids a set of device to device users to establish a safe device to device group session without seeping their identity privacy. It is protected against exterior cruel enemies with insubstantial processes. Official security enquiry and wide investigational exam displayed the security, proficiency and efficiency of their procedures [38].

There are new researchers presented a complete research on the security of 5G wireless systems compared to the customary mobile systems. They started with an analysis on 5G systems discriminations as well as on the unique requests and incentives of 5G network security. The possible bouts and refuge amenities are abridged with the deliberation of novel amenity necessities and modern use circumstances in 5G networks. The existing improvement and the current approaches for the 5G security are obtainable based on the equivalent security amenities, counting privacy, integrity, authentication, availability, key

management and data concealment. And discoursed the novel security topographies including diverse mechanisms practical to 5G system, such as massive MIMO, heterogeneous networks, D2D communications, IoT and SDNs. Striving by these security study and improvement actions, they proposed new 5G network security structural design, built on which the scrutiny of identity administration and malleable authentication is delivered. And they proved the AKA in 4G mobile systems is symmetric-key based. However, 5G network needs authentication between user equipment and mobile management entity and also between additional third parties such as service suppliers. As the faith typical varies from that used in the traditional mobile systems, flexible and hybrid authentication management is required in 5G. The flexible and hybrid authentication of user equipment could be applied in three diverse methods: authentication by both network and service supplier, authentication by network only, and authentication by service supplier only.

They discovered that in order to make little dormancy necessity of 5G systems, authentication methods are necessary to be extra effective in 5G than ever earlier. To influence the benefits of SDN a fast validation pattern in SDN is suggested, which usages are considered secure-context-information removal as a non-cryptographic safety system to advance validation effectiveness through great recurrent handovers in a HetNet in order to report the dormancy requisite [39].

On the other hand, other researchers declared that 5G appears to be accepting novel multi-party based ecologies where numerous performers can be collaborating in the overhaul supply.

This will involve the use standing and reliance contrivances knack to someway enumerate which performer is economically responsible for dilapidations or the amenity outages. Adding to that, 5G will intensely rely on softwarization replicas such as slicing, Software Defined Networking (SDN), and Network Functions Virtualization (NVF). Softwarization carries numerous defies into the table. They came to the conclusion that to achieve and confirm the refuge and flexibility of acute software objects while do not forget that the dynamicity of persons Softwarized substructures. To this end, they requisite intellectual mistake administration and extenuation threat schemes to do on the system at structure period and run-time. Softwarization increases subjects around the significance of a robust system authentication and robust portions segregation. And they suggested 5G systems as its precursors need to go through a regular of systems at the same time as confirming the privacy of users [40].

other researchers conducted a similar study to previous researches, however they studied correlated researches and presented SDN 5G network as a stage to support effective privacy protection and authentication handover as shown in figure (7).

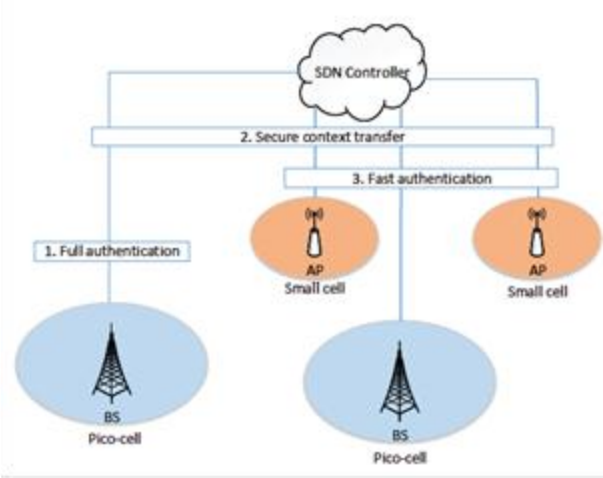

Figure 7: A SDN enabled authentication model [41].

Their impartial is to make simpler authentication handover by universal management of 5G HetNets by partaking of customer reliant security perspective information between linked access points. They demonstrated that SDN enabled security keys are extremely effectual through its consolidated mechanism competency, which is important for delay-embarrassed 5G communications.

They proposed that SDN would not only enable solution to provide a reconfigurable system administration stage, however, moreover streamlines validation handover in attaining abridged dormancy. The recital of the proposed outlines have been established by using specimens and mathematical simulations. They expected that extra development can be completed by using non-cryptographic methods and embryonic SDN enabled 5G construction to statement the 5G defies of abridged cell scope and concomitance of heterogeneous systems. Several fascinating linked areas, counting system complication, security presentation under diverse assaults, and operational use of security perspective information, could be exposed for SDN enabled 5G sanctuary contraptions [26].

Whereas there are new researchers provided a general idea of the security contests in SDN, NFV and clouds, and the contests of customer solitude. And they presented answers for these contests and upcoming instructions for protected 5G systems. They moreover believed in order to sanctuary the user privacy in 5G systems, there must be shared arrangements and reliance replicas amongst several participants complicated in the process such as application designer, network operator, user, service provider, and industrialist on information use and storing. For that, 5G technology will need improved method for subscribers actual individuality that might be concealed and changed by pennames [5,42].

Other researchers on the other hand, purpose is to extant essentials of user organized secrecy required for the upcoming 5G systems. They concluded that an ecology containing of a trusted third party between the service suppliers and termination user as a disseminated network might be combined to safe the viewpoint of precise privacy of subscriber for upcoming amenities.

They suggested the notion of a trusted third party that can purpose like a disseminated network between the service supplier and the customer. The trusted third party is not as such a straight slice of the upcoming 5G system however, a part of the communal features compactly attached with important necessities for 5G network and as a portion of the upcoming network substructure or ecology. By the trusted third party, there is a casual to

make simpler the customers' administration and regulation of their secretive information and that will be a stage in the correct path [43].

Whereas other researchers provided the complete official archetypal of a procedure from the authentication and key agreement group. They also removed exact requests from the 3GPP principles describing 5G and they identified disappeared security aims.

They conducted a complete, methodical, security estimation of the typical with reverence to the 5G security aims. Their automatic examination pinpoints the least security suppositions essential for every security aim and they found that some perilous security aims are not happened, excepting under supplementary expectations lost from the normal [44].

The researchers of the present study found that these ways aim to provide mutual entity authentication in 5G. They proposed a new verification protocol, with whole communal verification between the user equipment, the serving network as shown in figure (8).

The solution modified the authentication and key agreement protocol, and message elements, the SN and the UE and added new party like SDN and NVF. This is a significant operative disadvantage of it that the use of this method is necessary to the adjustment of the bodily level system that would prime to moving the hardware, that may be expensive.

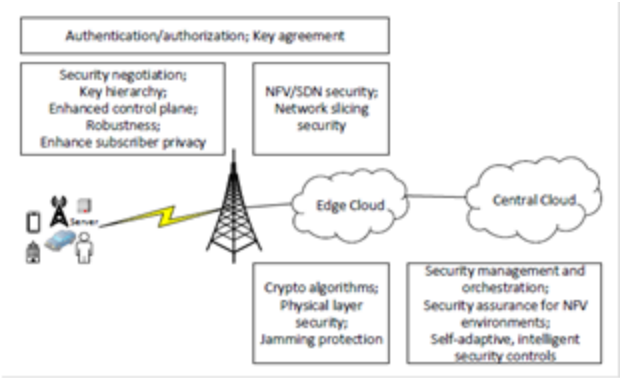

Figure 8: Elements in a 5G security architecture [45].

B- Proposed solutions for paging procedure

There is a study focused on paging procedure in 5 G network, those are researchers analyzed privacy facets of the paging process in a detailed manner and investigated the probability of a novel defense method which defends the IMSI in together preliminary fasten and paging processes.

They presented their examination and suggested improvements for paging process to defend the privacy of IMSI in both directions, in the uplink and in the downlink. They decorated privacy faintness in the present paging process and offered suggested developments, that are striking for existence accepted in upcoming 5G networks [31].

The researchers of the present study found that these ways are beneficial to alleviate privacy attacks against the paging procedure. However, every user equipment should check and decrypt all the conventional permanent identity paging and location update to decide if it is the beneficiary as shown in figure (9).

The competences of this method, a disadvantage of the use of this procedure

is the requisite to modification the physical level process that would result in modifying the hardware, which may be expensive. And the pseudonym may be recurrence more than one time in the same location area, and the size of IMSI will be large. If they used the same identity in attach and paging, the complexity will be more.

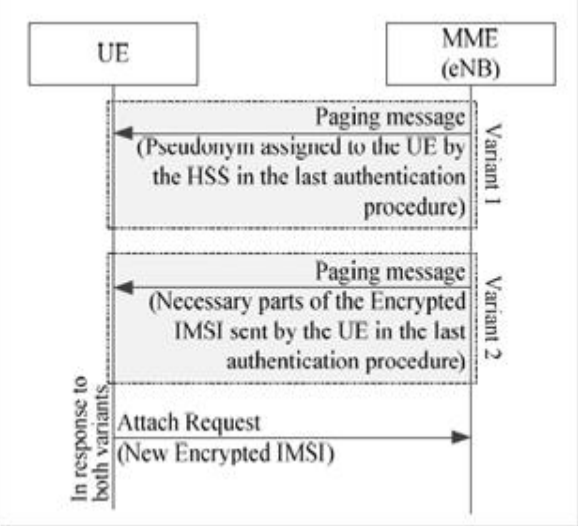

Figure 9: Simplified paging with privacy improvements [31].

C- Proposed solutions for location privacy

Different studies proposed solutions for location privacy among those are conducted researchers found that for example, a communication can be encrypted previously distribution to a location-based services supplier. Procedures such as complication are too central, where the feature of location information is abridged to make location privacy is defended. Furthermore, location-cloaking-based algorithms are somewhat suitable to grip various main location privacy assaults such as boundary and timing assaults [5,42].

Other researchers similar to previous researchers however, they analyzed the efficiency of cell actual to alleviate location privacy dangers in ultra-dense networks.

They inspected, as well, the influence on location privacy coming from assortment of both entrance nodules and portable nodules in the situation of ultra-dense networks. The sign from this research thoughts on the way to the knowledge that the further the vagueness of evidence about node-to-access-point sequential suggestions retrieved by an enemy is, the thornier location documentation responsibilities [46].

The researchers of the current research found that the suggestions to protect are located by using encryption either based location or service. While this is an stimulating technique to reservation privacy, one should inspect its applicability. The communication complexity and great calculation complication as a consequence of sending encrypted IMSI or C-RNTI. And the expanse of signaling overhead would be intolerable.

5. Conclusion

This paper presents the challenges of user privacy in 5G networks which contains identity privacy and location privacy, and discusses a number of researches that study the privacy of user in 5G and suggests the proposed solutions for permanent identity, paging and location privacy.

There are some authors who assumed that 5G is like 3GPP in authentication and AKA protocol, and others who assumed that the 5G will be new in architecture,

authentication and AKA protocol and suggested that SDN and NFV should be added to 5G security, while others shed light on the D2D and vehicular security. There are new proposals to dial with 5G which can enhance the privacy but there is no real implementation.

6. References

[1] Deliverable D2.2 Trust model, 5G-ENSURE. Available at: http://www.5gensure.eu/sites/default/ files/5GENSURE_D2.2%20Trust%20model% 20%28draft%29_v1.1.pdf

[2] J. Andrews et al., *"What Will 5G Be?"* IEEE JSAC, vol. 32, no. 6, pp. 1065–82, 2014.

[3] Deliverable D2.1 Trust model, 5G-ENSURE. Available at: http://www.5gensure.eu/sites/default /files/Deliverables/5G ENSURE_D2.1 UseCases.pdf.

[4] E. C. Jiménez, "Encrypting IMSI to improve privacy in 5G Networks," Master thesis, School of Information and Communication Technology School of Electrical Engineering KTH Royal Institute of Technology, 2017

[5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine*, Vol. 2, pp. 36-43, 2018.

[6] D. Fang, Y. Qian, and R. Qingyang Hu2, "Security for 5G Mobile Wireless Networks," *IEEE Access*, Vol. 6, pp.4850-4874, 2017.

[7] S. Farhang,Y. Hayel and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in *Conf. IEEE Conference on Communications and Network Security (CNS)*, Florence, Italy, 2015, pp. pp. 263-271.

[8] A. Muthana , M. Saeed , "Analysis of User Identity Privacy in LTE and Proposed Solution" *I. J. Computer Network and Information Security*, vol. 7, pp. 54-63, 2017.

[9] B. Woods, "3G flaw makes any device vulnerable to tracking,". ZDNnet[Online], 9 October 2012. Available: http://www.zdnet.com/article/3gawmakes-any-device.

[10] T. Doumi, M. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, " "LTE for public safety networks"," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 106-112, 2013.

[11] Ta T., Baras J.S." *Enhancing Privacy in LTE Paging System Using Physical Layer Identification*," in *Data Privacy Management and Autonomous Spontaneous Security*, Di Pietro R., Herranz J., Damiani E., State R, Eds. Lecture Notes in Computer Science, vol 7731. Springer, Berlin, Heidelberg, 2013, pp 15-28.

[12] 5G security, Ericson White paper Uen 284 23-3269, June 2017.

[13] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux, " "Security and privacy in next generation mobile networks: LTE and femtocells,"" in 2nd International Femtocell Workshop, Luton, UK. Citeseer, 2010, pp.65-68.

[14] " Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013– 2018, Cisco[Online], 2014.

Available" http://tinyurl.com/ b9berc.
[15] F. van den Broek, R. Verdult, and J. de Ruiter. "Defeating IMSI catchers," In Proc. of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2015, pp.65-68.
[16] H. Ghafghazi_, A. El Mougy, H. Mouftah, "Enhancing the Privacy of LTE-based Public Safety Networks: In Proc. 13th Annual IEEE Workshop on Wireless Local Networks, Edmonton, AB, Canada, 2014, pp. 753- 760.
[17] A. Ijaz, S. Namal, M. Ylianttila and A. Gurtov, "Security in software defined networks: a survey," *IEEE Communications Surveys and Tutorials*, vol.17, no. 4, pp. 2317–2346, 2015.
[18] K. Norrman, Xi' an, "Protecting IMSI and user privacy in 5G networks," In Pro. the 9th EAI International Conference on Mobile Multimedia Communications, 2004, pp. 159–166.
[19] 5G Security, Ericsson, White paper, Available at: https://www.ericsson.com/ res/docs/ whitepapers/wp-5g-security.pdf. June 2015.
[20] 5G Security: Forward Thinking Huawei, White paper. Available at: http://www.huawei. com/ minisite/5g/img/ 5G_Security_Whitepaper_en.pdf on Communications and Network Security (CNS).
[21] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User Privacy, Identity and Trust in 5G," in *A Comprehensive Guide to 5G Security* , M. Liyanage, I. Ahmed, A. b. Abro, A. Gurto, M. Ylianttila, Eds. John Wiley & Sons Ltd. 2018, pp. 267-279.
[22] D. Strobel. IMSI catcher. Ruhr University Bochum report, 13 July 2007. Retrieved 2016-04-07. https://www.emsec.rub.de/media/crypto/attachments/_les/2011/04/imsi catcher.pdf.
[23] K. Shubber. Tracking devices hidden in London's recycling bins are stalking your smartphone. Wired magazine [Online], 2013. Available: http://www.wired.co.uk/news/archive/2013
[24] A. muthana, M. Saeed, A. Abd Ghani, R. Mahmod, "Enhancing Privacy of Paging Procedure in LTE," *International Journal of Engineering Science Invention*, vol. 7, pp. 42-50, 2018
[25] Yu, R. et al. "A location cloaking algorithm based on combinatorial optimization for location-based services in 5G Networks," *IEEE Access*, vol. 4, pp.6515–6527, 2016.
[26] X. Duan and X. Wang "Authentication Handover and Privacy Protection in 5G HetNets Using Software-Defined Networking," *IEEE Communications Magazine*, vol.53, pp.28-35, 2015.
[27] K. Norrman, M. Näslund and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," in *Conf. 9th EAI International Conference on Mobile Multimedia Communications*, Xi'an, China, 2016, pp.159-166.
[28] M. Khan and V. Niemi," Concealing IMSI in 5G Network Using Identity Based Encryption," in *Network and System Security*, Y. Zheng, etal. Eds. Springer, 2017, pp.544-554.
[29] M. Khan and V.Niemi, "Privacy Enhanced Fast Mutual Authentication in 5G Network Using Identity Based Encryption," *Journal of Information and Communication Technology*, vol. 5, pp.69–90, 2017.

[30] P. Zhang, M. Durresi and A. Durresi, "Mobile Privacy Protection Enhanced with Multi-access Edge Computing," in *Conf. IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, 2018, pp. 724-731.

[31] E. C. Jiménez, P. K. Nakarmi, M. Näslund and K. Norrman, "Subscription identifier privacy in 5G systems," *in Conf. International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, Avignon, 2017, pp. 1-8.

[32] J. Arkko, K. Norrman, M. Näslund and B. Sahlin, "A USIM Compatible 5G AKA Protocol with Perfect Forward Secrecy," in *Conf. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015, pp. 1205-1209.

[33] M. Khan, V. Niemi & P. Ginzboorg, "IMSI-based Routing and Identity Privacy in 5G", in Conf. 22nd Conference of Open Innovations Association FRUCT, Helsinki, 2018, pp. 338-343.

[34] R. Rajavelsamy, D. Das and M. Choudhary, "Privacy protection and mitigation of unauthorized tracking in 3GPP-WiFi interworking networks," in *Conf. IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, 2018, pp. 1-6.

[35] S. Vij and A. Jain, "5G: Evolution of a secure mobile technology," in *Conf. 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 2192-2196.

[36] M. Hashem Eiza, Q. Ni and Q. Shi, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868-7881, Oct. 2016.

[37] A. Zhang and X. Lin, "Security-Aware and Privacy-Preserving D2D Communications in 5G," *IEEE Network*, vol. 31, pp. 70-77, 2017.

[38] M. Wang and Z. Yan, "Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3637-3647, Aug. 2018.

[39] 3GPP TS 23.401. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network; (E-UTRAN) access. Retrieved 2016-04-07.

[40] G. Arfaoui, J. M. S. Vilchez and J. Wary, "Security and Resilience in 5G: Current Challenges and Future Directions," in *Conf. IEEE Trustcom /BigDataSE/ICESS*, Sydney, NSW, 2017, pp. 1010-1015.

[41] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in *Conf. IEEE International Conference on Communications (ICC)*, Kuala Lumpur, 2016, pp. 1-6.

[42] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "5G security: Analysis of threats and solutions," in *Conf. IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, 2017, pp. 193-199.

[43] L. T. Sorensen, S. Khajuria and K. E. Skouby, "5G Visions of User Privacy," in *Conf. IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, 2015, pp. 1-4.

[44] D. Basin, J. Dreie, L. Hirschi, S.

Radomirović, R. Sasse and V Stettler, “A Formal Analysis of 5G Authentication,” in Conf. ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018, pp. 1383-1396.

[45]Security Challenges and Opportunities for 5G Mobile Networks, Nokia,Espoo, Finland, 2017.

[46] E. Catania and A. La Corte, "Location Privacy in Virtual Cell-Equipped Ultra-Dense Networks," in *Conf. 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, 2018, pp. 1-4.

journal homepage:www.ojs.sabauni.net

S.J.I.T.N Saba Journal of Information Technology and Networking

Article

A Comparative Study of Using Databases Technologies in Yemeni Organizations

Mohammed N. AL-khawlani

Department of Mathematics, Amran University, Yemen

Article info

Article history:

Accepted: March. 2019

Keywords:

DBs technologies, Yemeni Organizations, Organization Type, Type of Business

Abstract

Information Technology (IT) is having the kind of revolutionary, restructuring impact that makes major changes in the way of life and work. Database (DB) is the most important technology for any organization to provide and manage the information and knowledge. However, using databases technologies in the Yemeni organizations still a little compared to the most of organizations in the world.

This paper compares the usage of DBs technologies in the Yemeni organizations to evaluate and compare among these technologies. Further, this paper presents several reasons for none using one or more using DBs technologies in some of organizations. DBs technologies in this paper are Databases Management Systems(DBMS), Data Warehouses, Data Mining, and Enterprise Resource Planning(ERP). Data for this study are randomly collected from different organization's sectors based on organization type and type of business. This study was conducted by several steps: determining the DB technologies, proposing factors non using DB technologies, designing the questionnaire, distributing the forms of questionnaire on 115 big governmental and private companies and organizations , collecting the data based on 105 responses , and analyzing the data using SPSS application.

The results of this study show that the ERP technology has the lowest percentage (28%) of use. Further, more than 50% of organizations do not know ERP. In addition, 49.04%, 61.38% for Data Mining and Data warehouse respectively. In contrast, DBMs is used by most of organizations (95.24%).

* Corresponding author:
E-mail: Mnaser201435@gmail.com

1. Introduction

Information Technology (IT) is having the kind of revolutionary, restructuring impact that makes major changes in the way of life and work [5]. Database Technologies has quickly developed and growth since 1960s. Firstly, the focus was on automating the process, then moved to managing the corporate data, then to explore the knowledge from huge databases until reach to Data warehouse, ERP, and etc.

In Yemen, the first sector has used DBs technology is Telecommunications at first of 1980's, by Ministry of Telecommunications, to automate and compute the bells of home phones calls. In mid 1990's, use of database technology rapidly increased by several organizations, especially private sectors. Further, in this period, several companies for producing and developing DBs applications have established. However, the big number of companies stood look to DBs as not necessary because of the cost and culture. After 2000s, most of companies have concerned to buy and use databases applications. In contrast, the use of other DBs technologies such as *Data Mining*, *Data warehouse*, *ERP*, and *Web database* was very weak.

This paper compares the using DBs technologies in the Yemeni organizations and compare among them based on using these technologies. Further, this paper finds out several reasons for none using one or more DBs technologies by some of organizations. The DB technologies that are included in this paper are *DBMS, Data Warehouse, Data Mining,* and *ERP*. Data of this study are collected from different organization's sectors based on Organization Type and Type of Business. Organization Type includes *Governmental, Private*, and *Mixed*. Type of Business includes *Telecom &Technology*, *Health &Medicine*, *Education*, *Industry*, *Finance*, and *Other*.

2. Related work

[1] performed a survey on information society in Yemen. This survey includes the development in communications and Information technologies (ICT) sectors for several years starting 1990. This survey also includes other sectors that relate to ICT such as Human Resources and Departments of IT in the Yemeni Universities.

[2] Studied the market of Internet during the period 1996 until 2006 based on governmental reports especially for the Ministry of Communication and Information Technologies. Until April 2002, Y.net was the only Internet Service Provider. In April 2002, the second ISP that called Yemen Net was added. Based on Arab Advisor Group (AAG) report on February, 2006, the Internet penetration in Yemen is among the lowest in the Arab world region. Further, Yemen's grew at a CAGR of 87% between 2000 and 2005.

[3] produced a report on information society in Yemen. This report included the stages of developing ICT in Yemen during 15 years ago. The ICT sector has received considerable attention in Yemen. This attention was represented by preparing the infrastructure of ICT, developing the policies, plans and legal and regulatory frameworks, and etc.

[4] evaluated the use of E-commerce technologies such as E-payment, Websites, and emails in the Yemeni private organizations. Further, this work tried to find out the opportunities and challenges of

using e-commerce for the Yemeni private companies.

[7] studied and analyzed the market of internet in Yemen. It concluded that the penetration in Yemen is among the lowest in the Arab world region. In September 2005, Yemen's Internet subscribes penetration stood at a very small 0.5% and the internet users penetration was however 2.4%. The study provides, moreover, detailed and comprehensive picture on the Internet market strategies and regulations.

[8] made survey on using ERP in the UAE's companies. This survey included 342 senior managers, working for medium to large organizations. Based on survey, the most reason of using ERP is to have integrated system by 67%. Further, the most important factors for selecting ERP system is product functionality 56%, and product technology 52%.

[9] aims to examine the relationship between technology transfer performance and competitive advantage. Using the quantitative research approach, the theoretical model and hypothesized relationships among the variables were tested based on empirical data collected from 514 managers and engineers selected randomly from nine oil and gas companies in Yemen. The findings of this study show that with improvements in knowledge acquired from foreign companies, working practices, and long-term adoption of transferred technology, there is more inducement to establish competitive advantage by producing with low cost and high quality, especially in oil and gas industry.

[10]reviews other researches in the area of technology adoption in organizations in Yemen. In addition, this paper proposes a theoretical framework that takes into consideration the main factors that might affect technology adoption in organizations.

3. Data collection and preparation

Data of this study collected by questionnaires from 105 Yemeni organizations at the start of 2013 year. These organizations are randomly selected. This selection included the variant of fields of business and the main three sectors, governmental, private, and mixed. The number of selected organizations for each filed and sector is not firstly considered. Thus, the number of organizations for each sector and field is different about the other sectors and field based on the number of cases that got by the questioner. The collected data were analysed using SPSS version 11.5 for windows**.**

4. Results and discussion

The results of this study can be divided into groups based on the type of DB technology, organization type, and type sector. For the results based on the DBs technology, Table 1 shows the percentage of use for each technology.

Table 1. Percentages of using DBs Technologies in Yemen

DB Technology	Percentage of Use
Data Mining	49.04%
Data Warehouse	61.32%
ERP	28.00%
DBMS	95.24%
Average	58.40%

For more details, the percentages of using DBs technologies are based on the type of organization, *governmental*, *private*, and *mixed* are shown in Table 2.

Table 2. Percentages of Using DB Technologies Based on Organization Type

DB Technology	governmental	private	mixed
DBMS	100.00%	93.33%	100.00%
Data Mining	41.67%	52.70%	33.33%
Data Warehouse	50.00%	63.16%	83.33%
ERP	4.35%	36.62%	16.67%
Average	49.00%	61.45%	58.33%

Based on Table 2 and Figure 2, it is apparent that the highest average of using DBs technologies is for the private sector where as the lowest average is for governmental sector. It is worth mentioned that some percentages values 100 do not mean that all organization in this sector use this technology but this value depend on the number of chosen organizations from the sector in randomly way that use this technology.

For the results that based on the business sector, Table 3 shows the percentages of using each DBs technology in each business sector.

For Reasons of none use DB Technologies, several reasons are considered that may effect on none using any DB technology. These reasons are uninterested, costed, unknown, and other. Table 4 shows the most considered reasons.

Based on Table 4, the highest percentage of none use is for ERP (71%) where the most reason of none use this technology is unknown(50%) by the organizations.

In contrast, the lowest percentage of none use is for DBMS where this technology has become very necessary and more important in any organization to perform the most of works compared to the other DB technologies.

5. Conclusion

Based on the results of survey in this paper, the level of using DBs technologies is rapidly growth compared to the small age of information technologies in Yemen. Currently, most of the organizations in variant of business field and sectors use DBMSs to manage their works. In contrast, ERP, Data Mining, Data warehouse technologies still a little use where these technologies are not considered by the most of peoples and organizations in Yemen.

Table 3. Percentages of using DBs Technologies based on business sectors

DB Technology	**Telecom. & Technology**	**Health & Medicine**	**Education**	**Industry**	**Finance**	**Other**
DBMS	92.00%	100.00%	100.00%	100.00%	94.59%	95.24%
Data Mining	52.00%	60.00%	66.67%	100.00%	39.47%	48.00%
Data Warehouse	52.00%	70.00%	66.67%	100.00%	60.53%	62.96%
ERP	45.83%	60.00%	0.00%	0.00%	22.86%	13.64%
Average	**60.46%**	**72.50%**	**58.34%**	**75.00%**	**54.36%**	**54.96%**

Table 4. Reasons of none using DBs technologies

DB Technology	Uninterested	Costed	Unknown	Other	Total	% of None Use
Data Mining	18	3	22	9	52	50.96%
Data Warehouse	11	5	15	9	40	38.68%
ERP	10	5	50	6	71	72.00%
DBMS	2	0	1	2	5	04.76%
Average	**10.25**	**3.3**	**22**	**6.5**	**42**	**41.60%**

The most reason of none using these technologies is unknown especially ERP by the most of organizations may for several reasons, the low level of education, boor sense and knowledge of important these technologies by Chief information officers(CIOs) in the organizations, and the culture of people in Yemen.

For future works, there are several issues are concerned to will be done. First, it is concerned to survey and evaluate the use and none use of web-database, Decisions support systems (DSS) technologies. The second issue is evaluating the level of database security and the challenges that face in the Yemen's organizations for protecting own information.

6. References

[1] ESCWA-ICTD, "National Profile of the Information Society in Yemen. United Nations," New York, 2009.

[2] M. AS-SALOOL, "E-Commerce in Yemen: Opportunities and Challenges for Private Companies," Master thesis, OU University, Malaysia, 2009.

[3] ESCWA, "National Profile of the Information Society in Republic of Yemen," United Nations, New York, 2007.

[4] Kenny Bridgeson, *Information System Management*, 1st edition, Lotus press, 2006.

[5] Arab Advisor Group. Yemen's Internet market registers high growth rates. Yemen, 2006.

[6] Johannesburg. (22, Mar, 2006). ERP helps companies in the GCC come of age [Online]. Available: https://www.itweb.co.za/content/o1Jr5qxjw3n7KdWL

[7] A. H. S. Zolait, A. Sulaiman , and S. F. S. Alwi, "Prospective and challenges of internet banking in Yemen: an analysis of bank websites," International Journal of Business Excellence, vol. 1, 2008, pp. 353-374.

[8] Ado Ali Abdullah, "Factors Influencing Intention of Yemenis to Adopt Internet Banking," Master Thesis, UUM, Malaysia,2010.

[9] M. S. Al-Abed1, Z. A. Ahmad, M. A. Adnan, "Technology Transfer Performance and Competitive Advantage Evidence from Yemen," *Asian Social Science*, vol. 10, pp. 195-204, 2014.

[10] M. S. S. Al-Tuhaifi, "Factors Influencing Acceptance of Technology in Context of Yemen: Review," *American Journal of Computer Science and Information Engineering*, vol. 4, pp. 1-6, 2017.

[11] ISOC-Yemen Chapter, "E-Commerce in Yemen," v. 1.0. March-2016.

journal homepage:www.ojs.sabauni.net

Article

Dynamic Quantum Time Round Robin Scheduling Algorithm

Eman Al-Ariqi , Mohanad AL_Meshrekey
Department of Information Technology, Yemen Academy for Graduate Studies, Yemen

Article info

Article history:

Accepted: JUN. 2019

Keywords:
Round Robin scheduling algorithm (RR) , Time Quantum (TQ), Dynamic TQ , Scheduler; Dispatcher , FCFS , SJF , Schedule, Operating System

Abstract

Processor scheduling algorithms aim at organizing the entry of processes into the processor. The Round Robin (RR) algorithm which is the most frequently used algorithm, has been developed to give the less waiting time and a faster response time comparing to the First-Come-First-Served FCFS and Shortest Job First (SJF) scheduling algorithms. The performance analysis of these three algorithms shows that RR is similar to FCFS except that preemption is added to switch between processes. However, due the fixed quantum time unit assigned per process, RR may suffer a high turnaround and waiting time.

This paper presents a dynamic Quantum Round Robin algorithm that dynamically generates Quantum time units based on Burst time values for queues.

* Corresponding authors:
E-mail: eman.ahmed.yemen@gmail.com

1. Introduction

Task scheduling is a function of the operating system that Schedules process and optimally assign the required resources to them. It defines the required tasks and resources available from the processor, memory and devices at each point in time and distributes the required tasks in a way that makes the work faster, using some of the
FCFS scheduling algorithms, SJF, Priority, RR [6,8].

CPU scheduling deals with the problem of choosing a process from the ready queue to be executed by the CPU. The following the main CPU scheduling algorithms include :

First-Come-First-Served (FCFS)[8, 9] is the simplest scheduling algorithm, it simply queues processes in the order that they arrive in the ready queue (i.e waiting queue). Processes are dispatched according to their arrival time on the ready queue. Being a non-preemptive discipline, once a process has a CPU, it runs to completion. The FCFS scheduling is fair in the formal sense or human sense of fairness but it is unfair in the sense that long or unimportant jobs may make short jobs and unimportant jobs may make important jobs wait for long time [2, 5].

Shortest Job First (SJF) [2, 9] is the strategy of arranging processes with the least estimated processing time remaining to be the next one in the queue. It works under the two schemes (preemptive and non-preemptive). SJF provably optimal since it minimizes the average turnaround time and the average waiting time. The main problem with this discipline is the necessity of the previous knowledge about the time required for a process to complete. For theme, it undergoes a starvation issue especially in a busy system with many small processes being run [2, 5].

Round Robin (RR) [8, 9]which is the main concern of this research is one of the oldest, simplest and fairest and most widely used scheduling algorithms, designed especially for time-sharing systems. It's designed to give a better responsive inters but the worst turnaround and waiting time due to the fixed time quantum concept. The scheduler assigns a fixed time unit (quantum) per process usually 10-100 milliseconds, and cycles through them. RR is similar to FCFS except that preemption is added to switch between processes [2, 3, 4,15].

RR is the most common and used, each scheduling algorithm has its advantages and disadvantages. Similarly, the RR faults give it the largest average waiting time and the mean response time less through a fixed time called Quantum.[14]

1.1 SCHEDULING CRITERIA

There are different scheduling algorithms and performance of each can be judged on various criterions. Different algorithms may favor different types of processes. Some criteria are as follows:

- CPU Utilization: Amount of time till CPU remains as busy as possible.
- Throughput: Number of processes that complete their execution per unit time.
- Burst Time: Amount of time required for the process for its execution.
- Completion Time: The time when process completes its execution.
- Turnaround Time: The time required to execute a particular process. It is denoted by:

  Turnaround Time= Completion

Time - Arrival Time

- Waiting Time: Amount of Time process was waiting in waiting queue. It is denoted by:

Waiting Time= Turnaround Time - Burst Time

Response Time: Amount of time from the submission of a request until the first response is produced.[6,16]

1.2 Motivation

In RR scheduling, operations get a fixed amount of CPU due to a fixed quantum time. The processes are entered into the processor at equal time by Quantum. The process returns to the waiting queue if it is not completed. Similarly, the rest of the operations are entered End it.

The catalyst was the Quantum factor where it was able to improve the performance of this algorithm if it was generated dynamically and also we needed to know which of the scheduling algorithms are considered the best in reducing and waiting.

2. Related work

IMRRSJF [5] algorithm uses mean and highest burst time to calculate the time quantum. Sort the ready queue in ascending order according to processes' burst time. Calculate the time quantum using mean and median. If mean is greater than median then time quantum is equal to ceil(sqrt((mean * highest burst time)+(median*lowest burst time))) and if median is greater than mean then time quantum is equal to ceil(sqrt((median * highest burst time)+(mean*lowest burst time))) otherwise time quantum is equal to mean [6]. Adaptive Round Robin [7] is a novel approach based on Shortest Burst Time using Smart Time Slice. Sort the processes according to their burst time and calculate Smart Time Slice. Smart Time Slice is equal to mid process burst time of all the CPU burst time when number of process given odd and if number of process given even then time quantum is chosen according to average CPU burst time of all running processes. In [8], processes in the ready queue are sorted in ascending order according to processes' burst time and time quantum is computed with the help of median and highest burst time. In [9], Time Slice is equal to the median of all the sorted processes present in ready queue. Time slice is recalculated taking the remaining burst time in account after each cycle. Enhanced Round Robin [10] scheduling algorithm allocates the processor to the first process of the ready queue for a time interval of up to 1 time quantum. Then it checks the remaining burst time of the currently running process and if the remaining burst time is less than or equal to 1 time quantum, the processor again allocated to the same process. Behera et. al [11], [13] devised a method for determining time quantum based on where a process lies in a list ordered based on burst time length. Their method involves setting a time quantum for processes with lower burst times to a median burst time for those processes, then for every process in the upper quartile of burst times, assign a time quantum equaling the sum of all burst times above the median. Panda and Boi [12] devised a method that achieved lower turnaround time, average waiting time, and number of context switches by adjusting the time quantum during each cycle using Mix-Max dispersion in accordance with each process's remaining burst time.

3. The Proposed Algorithm (IRRWDQ)

The proposed algorithm is comprised of some steps as following:

Step 1: Enter process name, Arrival time and burst time.

Step 2: Store the above details in a queue called READYQ

Step 3: The scheduler starts by inserting the parameters into the processor depending on and from the access and according to the Quantum time selected by the algorithm

$$(\text{IRRWDQ} = n + LNIBT + \frac{\text{HNIBT}}{2}).$$

HNIBT = High Number In Burst Time .

LNIBT = Low Number In Burst Time .

N= Number of Burst time .

Step 4: Update Burst time for operations .

Step 5: Return the unfinished operations and their implementation to the waiting queue again and return to step 3.

Step 6: Configure the Gantt Chart for the processes that are entered into the wizard

Step 7: The Average Waiting Time Average Completion time for all processes that are entered for the processor.

Step 8: It introduces new processes to the processor and returns to execution from the first step .

4. The Experiment

4.1. Data set

Table 1 shows the data set that is used in this study.

Table 1. scheduling data set

Process	Arrival Time (milliseconds)	Burst Time (milliseconds)
P1	0	28
P2	2	35
P3	6	50
P4	6	82
P5	8	110

4.2. Experimental environment

This Experimental was performed on the Core i5 processor type computer The memory was 6 GB and the type of Windows 8 .

4.3. Experimental results

Each algorithm was implemented separately. We implemented the first FCFS algorithm. The results were as shown in Table 2. We also implemented the second SJF algorithm. The results were as shown

in Table 3. We also implemented the third Round Robin algorithm. Results as shown in Table 4 and finally we have implemented the algorithm we have proposed Improved Round Robin With Dynamic Quantum as shown in Table 5.

Table 2: first come first serve (FCFS)

Process	Arrival Time (milliseconds)	Burst Time (milliseconds)	Waiting time	Turned around time
P1	0	28	0	28
P2	2	35	26	61
P3	6	50	57	107
P4	6	82	107	189
P5	8	110	187	297

Table 3: shortest job first (SJF)

Process	Arrival Time (milliseconds)	Burst Time (milliseconds)	Waiting time	Turned around time
P1	0	28	0	28
P2	2	35	26	61
P3	6	50	57	107
P4	6	82	107	189
P5	8	110	187	297

Table 4: round robin (RR)

Process	Arrival Time (milliseconds)	Burst Time (milliseconds)	Waiting time	Turned around time
P1	0	28	96	124
P2	2	35	120	155
P3	6	50	151	201
P4	6	82	185	267
P5	8	110	187	297

Table 5: improved round robin with dynamic quantum (IRRWDQ)

Process	Arrival Time (milliseconds)	Burst Time (milliseconds)	Waiting time	Turned around time
P1	0	28	0	28
P2	2	35	0	35
P3	6	50	35	85
P4	6	82	85	167
P5	8	110	167	277

Table 6: results of comparison between scheduling algorithms

Algorithm	Average Turn Around Time (milliseconds)	Average Waiting Time (milliseconds)
FCFS	136.4	75.4
SJF	136.40	75.40
RR	208.8	147.8
IRRWDQ	118.4	57.4

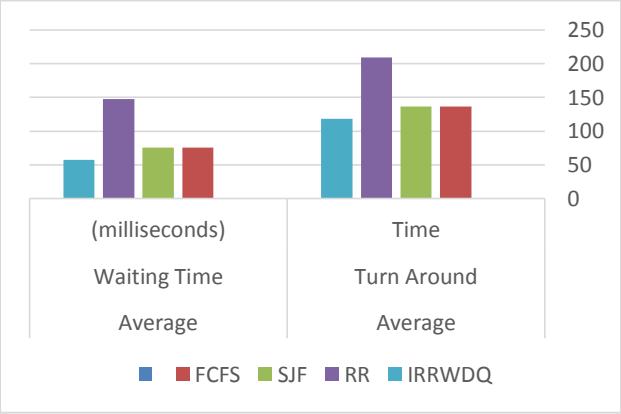

Figure 1. Results of comparison between scheduling algorithms

The results of the FCFS algorithm and the SJF algorithm were equal in terms of implementation time and completion time because the order of entry to the processor was the same as the order of the two algorithms. The RR algorithm was high, so we modified this algorithm and proposed our new IRRWDQ algorithm, We reached it.

5. Discussion

The previous rule is calculated to calculate Quantum time based on the number of processes that will be entered into the processor in the queued queue and we collect them at the highest Burst time present among the expected operations and we also collect them with less Burst time divided by 2 and this code can generate dynamic Quantum time .

The following table shows the algorithms that were introduced to the processor, how long it was accessed and the time it was executed. It also shows Average Waiting time and Turned around time. This algorithm is the best in obtaining results. It reduces average waiting time and turned around time.

6. Conclusion

We conclude that the best algorithm in which we obtained the least waiting time and the least complete time before the development process is the FCFS algorithm, but after the development process of the RR algorithm by obtaining Quantum automatically by the previous code we got the best results through the algorithm we developed Improved Round Robin With Dynamic Quantum (IRRWDQ) .

In our work we improved RR through an

equation that calculates Quantum dynamically and appropriately for the processes in the queue to enter the processor and thus gave a better result in response time and waiting time.

This algorithm can be developed as a future work, which is to make Quantum time automatically generated depending on processor specifications and memory. Quantum generation will be better when it depends on the type of device and its specifications.

7. References

[1] A. Silberschatz, P. B. Galvin, G. Gagne, *Operating Systems Concepts*, 7th edition, Wiley publication, 2005.

[2] Silberschatz ,Galvin and Gagne, *Operating systems concepts*, 8th edition, Wiley, 2009.

[3] D. Nayak , S. Kumar Malla , D. Debadarshini," Improved Round Robin Scheduling using Dynamic Time Quantum, " *International Journal of Computer Applications* , vol. 38, pp.34-38 ,2012 .

[4] K. ElDahshan, A. A. Elkader, N. Ghazy, "Round Robin based Scheduling Algorithms, A Comparative Study," *Automatic Control and System Engineering Journal*, vol. 17, pp.1-11, 2012.

[5] R. Shyam, S. K. Nandal, "Improved Mean Round Robin with Shortest Job First Scheduling," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.4, pp. 170-179, 2014.

[6] Raman, Dr. P. Kumar Mittal, "An Efficient Dynamic Round Robin CPU Scheduling Algorithm," *International Journal of Advanced Research in Computer Science and Software engineering*, vo. 4, pp. 906- 910, 2014.

[7] V. K. Dhakad1, L. Sharma, "Performance Analysis of Round Robin Scheduling using Adaptive Approach based on Smart Time Slice and comparison with SRR," *International Journal of Advances in Engineering & Technology*, vol. 3, pp.333-339, 2012.

[8] P. S. Varma," A Best possible Time quantum for Improving Shortest Remaining Burst Round Robin (SRBRR) Algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, 2012.

[9]. H. S. Behera, R. Mohanty, D. Nayak, "A New Proposed Dynamic Quantum with Re-Adjusted Round Robin Scheduling Algorithm and its Performance Analysis," *International Journal of Computer Applications*, vol. 5, pp.10-15 ,2010 .

[10] J. Khatri, "An Enhanced Round Robin CPU Scheduling Algorithm," *IOSR Journal of Computer Engineering*, vol.18, pp. 20-24, 2016.

[11] Behera, H. S. et al. "Design and Performance of Multi Cyclic Round Robin (MCRR) Algorithm using Dynamic Time Quantum," *Journal of Global Research in Computer Science*, vol.2, pp. 48-53, 2011.

[12]. P. S. K. et al. "An Effective Round Robin Algorithm using Min-Max Dispersion Measure," *International Journal on Computer Science and Engineering*, vol. 4 pp.45-53, 2012.

[13] Behera, H. S. et al. "Comparative Performance Analysis of Multi-Dynamic Time Quantum Round Robin (MDTQRR) Algorithm with Arrival Time". *Indian Journal of Computer Science and Engineering*, vol.2 , pp. 262-271, 2011..

[14] Z. Bedell , A Olmsted," An Alternative Round Robin CPU Scheduling Algorithm with Average Burst Time-Dependent Time Quantum".

[15]K. ElDahshan, A. AEl-kader, NermeenGhazy, "Achieving Stability in the Round Robin Algorithm", *International Journal of Computer Applications*, vol.172 , pp.15-20, 2017.