International Journal of Research (IJR)

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

IMPROVING SECURITY AND RELIABILITY IN MOBILE NETWORK THROUGH VHAHA ARCHITECTURE

Kartik Goyal, Research Scholar

Aseem Gupta, Research Supervisor

Department of Computer Science and IT, Sunrise University, Alwar (Raj) INDIA

INTRODUCTION

Mobile network security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. New threats demand new strategies as the network is the door to your organization for both legitimate users and would-be attackers. For years, IT professionals have built barriers to prevent any unauthorized entry that could compromise the organization's network. And this network security is important for every network designing, planning, building, and operating that consist of strong security policies. The Network Security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape For example, the widespread adoption of cloud computing, social networking and bring-your-own-device (BYOD) programs are introducing new challenges and threats to an already complex network.

SECURITY GOALS FOR WIRELESS NETWORK

Survey on Security for Smartphone Device

The technological advancements in mobile connectivity services such as GPRS, GSM, 3G, 4G, Blue-tooth, WiMAX, and Wi-Fi made mobile phones a necessary component of our daily lives. Also, mobile phones have become smart which let the users perform routine tasks on the go. However, this rapid increase in technology and tremendous usage of the smartphones make them vulnerable to malware and other security breaching attacks.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

General Architecture of Smartphones

Smart devices are grouping of mobile phones and platform with rich connectivity and powerful computing proficiency. Therefore, a smart phone has the necessary modules of computing platforms, operating systems, third-party applications and smart phone hardware architectures, as shown in Unlike Android, the iOS operating system works only on iPad, iPhone, and iPod devices. To manage all operating systems and devices, the OS provide necessary technology and interface and support to implement the new application to meet a variety of smart phone user needs devices by interacting with the operating system, by such interaction users can access and control data communication interfaces and services.

On another hand, the operating system can access user data and communicate directly with other services as well as devices. In general operating system can only access hardware directly, but the access to user's data might result in compromising user information and the information from the smart phone can be maltreated by attackers just like attacks on the computer such as viruses, Trojans, etc. The user data or information is the most valued property of smartphones. As discussed earlier, besides communication, smartphones connect to several other electronic devices such as computer and even servers through the Internet. The data without user's knowledge is usually retrieved through the applications infested by malicious codes or programs.

Structure of Smartphones Operating System

Security for 5G Mobile Wireless Networks

5TH generation wireless systems, or 5G, are the next generation mobile wireless telecommunications beyond the current 4G/International Mobile Telecommunications (IMT)- Advanced Systems. 5G wireless system is not only an evolution of the legacy 4G cellular networks, but also a system with many new service capabilities. 5G research and development aim at various advanced characteristics, such as higher capacity than current 4G, higher density of mobile broadband users, and supporting device-to-device (D2D) communications and

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

massive machine-type communications. 5G planning also aims at lower latency and lower energy consumption, for better implementation of Internet of Things (IoT).

SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS

MANET is a kind of Ad Hoc network with mobile, wireless nodes. Because of its special characteristics like dynamic topology, hop-by-hop communications and easy and quick setup, MANET faced lots of challenges allegorically routing, security and clustering. The security challenges arise due to MANET's self configuration and self-maintenance capabilities. In this study, we present an elaborate view of issues in MANET security. Based on MANET's special characteristics, we define three security parameters for MANET. In addition we divided MANET security into two different aspects and discussed each one in details. A comprehensive analysis in security aspects of MANET and defeating approaches is presented. In addition, defeating approaches against attacks have been evaluated in some important metrics. After analyses and evaluations, future scopes of work have been presented.

In these years, progresses of wireless technology and increasing popularity of wireless devices, made wireless networks so popular. **Mobile Ad Hoc Network (MANET)** is an infra structure independent network with wireless mobile nodes. MANET is a kind of Ad Hoc networks with special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications. These characteristics of MANET made it popular, especially in military and disaster management applications. Due to special features, wide-spread of MANET faced lots of challenges.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

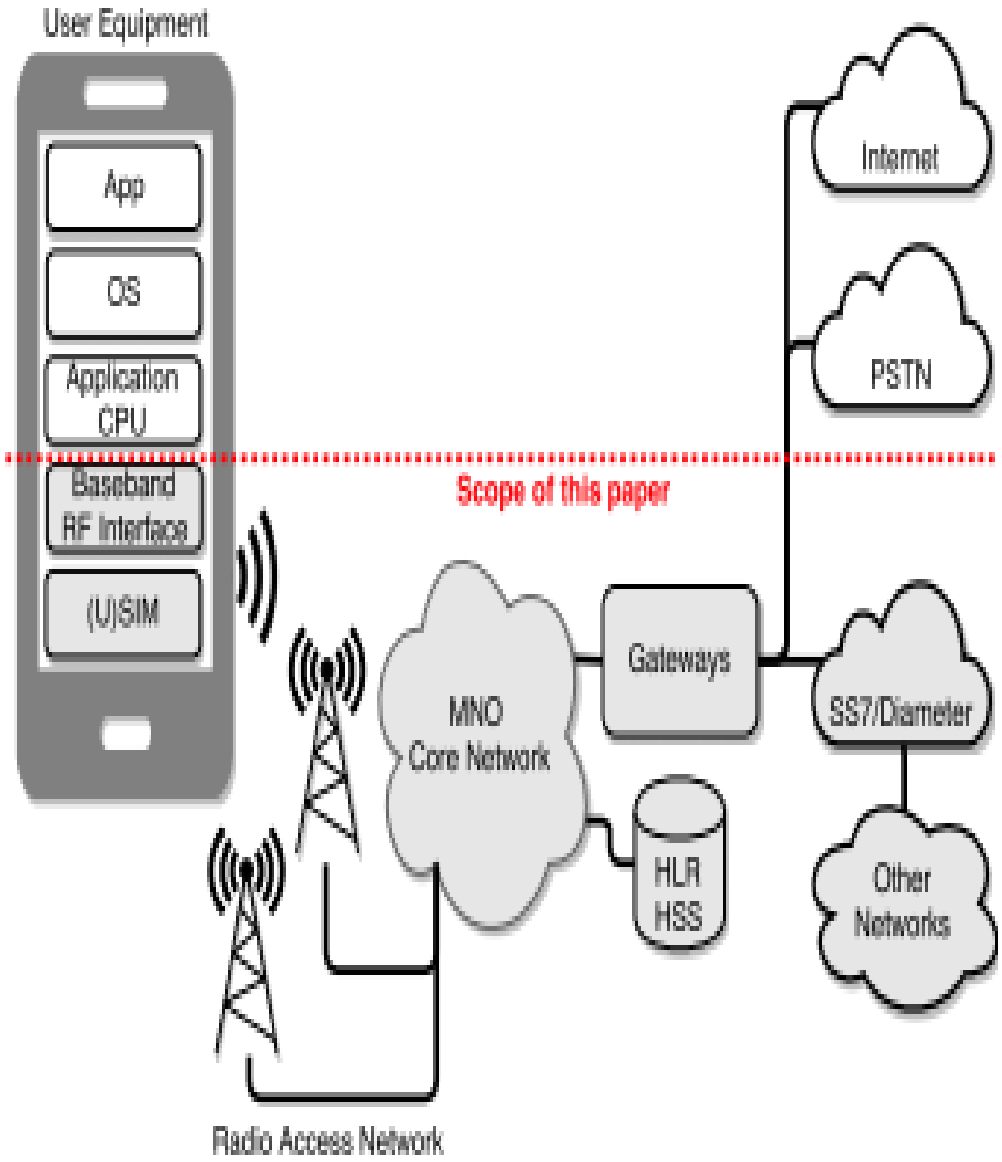

Figure:1 Generic Mobile Network Architecture and its Scope

REVIEW OF LITERATURE

David Rupprecht (2015) Over the last decades, numerous security and privacy issues in all three active mobile network generations have been revealed that threaten users as well as network providers. In view of the newest generation (5G) currently under development, we now have the unique opportunity to identify research directions for the next generation based on existing security and privacy issues as well as already proposed defenses. This study aims to unify security knowledge on mobile phone

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

networks into a comprehensive overview and to derive pressing open research questions. To achieve this systematically, we develop a methodology that categorizes known attacks by their aim, proposed defenses, underlying causes, and root causes. Further, we assess the impact and the efficacy of each attack and defense.

Vishal Sharma (2012) Cellular Communication has become an important part of our daily life. Besides using cell phones for voice communication, we are now able to access the Internet, conduct monetary transactions, send text messages etc. using our cell phones, and new services continue to be added. Therefore, it is important to provide users with a secure channel for communication. This survey study will give a brief introduction to the various generations of cellular networks. For those not familiar with the cellular network architecture, a brief description of the new 3G cellular network architecture will be provided.

T. Schulz, (2011) Mobile IPv6 will be an integral part of the next generation Internet protocol. The importance of mobility in the Internet gets keep on increasing. Current specification of Mobile IPv6 does not provide proper support for reliability in the mobile network and there are other problems associated with it. In this study, we propose **Virtual Private Network (VPN) based Home Agent Reliability Protocol (VHAHA)** as a complete system architecture and extension to Mobile IPv6 that supports reliability and offers solutions to the security problems that are found in Mobile IP registration part.

W. Kastner, (2015) the wireless network develops is support mobility within the Internet at presently. The mobile Internet use Mobile IP technologies in the wireless Internet. This study is concerned with the security aspect of the registration protocol in Mobile IP. In this study we publish a new method use the secure-key combine minimal public-key besides produce the communication session key in mobile node registration protocol. The all communication message are encrypt in our propose method. An easy and fast authentication method for establishing a mobile node's identity that can also prevent replay, TCP spicing and guessing attack is proposed.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

P. Nappey, (2012) Health information network security needs to balance exacting security controls with practicality, and ease of implementation in today's healthcare enterprise. Recent work on 'nationwide health information network' architectures has sought to share highly confidential data over insecure networks such as the Internet. Using basic patterns of health network data flow and trust models to support secure communication between network nodes, we abstract network security requirements to a core set to enable secure inter-network data sharing.

Snchez-Picot, (2016) The core network's task is to manage the connection mobility and to deliver the services, e. g., phone calls and Internet connection. For this mobility management, several core network elements are utilized. A central database, the Home Location Register (HLR) 2G or Home Subscriber Server (HSS) 3G,4G, stores the authentication, mapping, and other information about the users. Its security functionality is often referred as Authentication Center (AuC). Core network elements manage the mobility, connection, and security establishment.

D. Martín et al., (2015) First entity that can disrupt Mobile IPv6 based communication is the Mobility Anchor point itself, i.e. Home Agent Reliability of Home Agent is addressed first because if this mobility agent is not reliable there would be no reliability of mobile communication. Next scenario where mobile communication can get disrupted is created by MN itself and it is due to its mobility.

ANALYSIS

Cell Communication has turned into a significant piece of our day by day life. Other than utilizing phones for voice correspondence, we are currently ready to get to the Internet, lead money related exchanges, send instant messages and so forth utilizing our PDAs, and new administrations keep on being included. Be that as it may, the remote medium has certain constraints over the wired medium, for example, open access, restricted transmission capacity and frameworks intricacy. These impediments make it troublesome albeit conceivable to give security highlights, for example, verification, respectability and privacy. The present age of 3G systems have a bundle exchanged center which is associated with outside systems, for example, the

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

Internet making it helpless against new kinds of assaults, for example, refusal of administration, infections, worms and so on that have been utilized against the Internet.

Neural network chaotic encryption algorithm in communication

There are two kinds of chaotic models of neural networks. One is a neural network chaotic model based on artificial neurons. The corresponding equations are shown in Eq. 1, Eq. 2, and Eq. 3. The other is a cell-based neural network model based on unit cells. The essence is a hybrid nonlinear circuit composed of a linear circuit and a nonlinear circuit, and the corresponding equations are shown in equations:

$$xi(t)=11+e-yi(t)/\varepsilon xi(t)=11+e-yi(t)/\varepsilon \quad (1)$$

$$yi(t+1)=kyi(t)+\alpha(\sum j=1,j\neq inwijxj(t)+Ii)yi(t+1)=kyi(t)+\alpha(\sum j=1,j\neq inwijxj(t)+Ii) \quad (2)$$

$$zi(t+1)=(1-\beta)zi(t)(i=1,2,3\ldots n)zi(t+1)=(1-\beta)zi(t)(i=1,2,3\ldots n) \quad (3)$$

$$xij=-xij+\sum C(k,i)\in st(i,j)A(i,j;k,l)*ykl+\sum C(k,i)\in st(i,j)B(i,j;k,l)*UM+zjxij=-xij+\sum C(k,i)\in st(i,j)A(i,j;k,l)*ykl+\sum C(k,i)\in st(i,j)B(i,j;k,l)*UM+zj \quad (4)$$

$$yij=f(xi)=12|xij+1|-12|xij-1|yij=f(xi)=12|xij+1|-12|xij-1| \quad (5)$$

Disordered neural systems likewise have turbulent pulling in elements, which portray a specific condition of system task, which is the soundness factor of the system. It is the principle inward main impetus for the disordered wonder of neural systems. The use of disorderly neural system encryption calculation in correspondence for the most part has the accompanying three:

1. The application of chaotic synchronization based on the characteristics of encryption communication is mainly represented by the fourth generation chaotic pulse synchronous encryption communication. The theoretical basis is the Chua's oscillator, and its equation can be expressed as shown in equation:

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

x=a[y−x−f(x)]y=x−y+zz=−by−cz{x=a[y−x−f(x)]y=x−y+zz=−by−cz

(6)

where *a*, *b*, and *c* are constants and *f*(*x*) is a piecewise function of the Chua diode, and its correspondence can be expressed as in equation:

f(x)=dx+12(g−d)(|x+1|−|x−1|)f(x)=dx+12(g−d)(|x+1|−|x−1|) (7)

1. The application of chaotic sequences in encrypted communication is mainly based on the non-periodicity of sequence traces output by chaotic networks. The characteristics of nonlinearity and randomness, which cannot be accurately predicted, make it have the characteristics of being the main key, so that the approximate “one time, one secret” full confidentiality requirement can be guaranteed.
2. The application of chaotic factor-based neural network encryption in communication is mainly based on chaotic attractors.

Basic principle analysis and optimization algorithm

The traditional neural network chaotic encryption algorithm derives its algebraic structure from chaotic dynamics, chaotic attractors, and structural features of the attracting domain. The traditional neural network chaotic encryption algorithm is based on the chaotic attractor in the saturated Hopfield neural network as the relationship between the key and the ciphertext. The final result is a chaotic neural network-based security compared with the traditional encryption algorithm. The public key encryption algorithm, whose corresponding neural network energy function, is shown in equation:

E(t)=−12∑ijTijSi(t)Sj(t)E(t)=−12∑ijTijSi(t)Sj(t) (8)

A monotonic decrease in the energy function will cause the steady state of the entire algorithm to occur, and this steady state is also called an attractor. The corresponding algorithm flow chart is shown in figure.

The initial phase in the encryption procedure is to decide the key, which is gotten by changing the enormous framework. It requires each gathering of correspondence

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

clients to choose a joint neurotransmitter grid to shape a particular framework with a coefficient m. A change network is arbitrarily chosen in the m lattice, so the client can join the private key of the client with the open key of the data trade to acquire an open key between one another.

The substance is that the coding of each piece is legitimately created by the straightforwardly influenced code, and the relating recipe is produced. For equation:

code[i]=(code[i]+code[i−j]%range)code[i]=(code[i]+code[i−j]%range)

(9)

For the above-mentioned network composed of 8 neurons, the probability of the corresponding ciphertext change will be increased as shown in equation and the optimization algorithm proposed in this study is used for encryption processing:

prob(cipher)=prob(domain)(dim+(1/8)∗dim∗nn)+prob(domain)prob(code)prob(cipher)=prob(domain)(dim+(1/8)∗dim∗nn)+prob(domain)prob(code)

(10)

The probability of the corresponding impact on the ciphertext after adding the hybrid coding is as shown in equation:

prob(code)=min(prob(X0)+prob(X1)+…prob(Xi))∗dim−1dimprob(code)=min(prob(X0)+prob(X1)+…prob(Xi))∗dim−1dim

(11)

EFFICIENCY ANALYSIS

In this study, we select a data below 5M in the efficiency test direction to compare the encryption test of the algorithm before and after the improvement. The corresponding comparison table of encryption efficiency in PDF file mode is shown in Table;

Table: 1 The Corresponding Comparison Table of Encryption Efficiency in PDF File Mode

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

Testing frequency	Optimization algorithm proposed in this study (seconds)	Traditional algorithm (seconds)
1	17	15
2	14	14
3	16	17
4	17	17

The corresponding encryption efficiency corresponding to the TXT file mode is shown in Table 2;

Testing frequency	Optimization algorithm proposed in this study (seconds)	Traditional algorithm (seconds)
1	7.9	6.1
2	6.4	6.5
3	6.3	6.4
4	6.9	6.2

It can be clearly seen from the above tables that the improved algorithm is superior to the conventional algorithm.

SECURITY ISSUES IN CELLULAR NETWORKS

The infrastructure for cellular networks is massive, complex with multiple entities coordinating together, such as the IP Internet coordinating with the core network. And therefore, it presents a challenge for the network to provide security at every possible communication path.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

Wireless Application Protocol (WAP)

Since one of the most important services provided by 3G systems is access to the Internet, it is important to understand the security mechanisms of the protocol used to access the Internet. WAP is an open specification which enables mobile users to access the Internet. This protocol is independent of the underlying network e.g. WCDMA, CMDA 2000 etc and also independent of the underlying operating system e.g. Windows CE, PALM OS etc.

RESULT AND DISCUSSION

The main problems are mainly reflected in mobile terminal problems, communication link problems, and authentication system problems. The authentication system problem is communication security problem. Wireless communication security issues are not only related to people's privacy and security, but also related to people's property security when conducting currency transactions on the network and even related to national defense security. The key to solving the security problem of wireless network communication lies in the application of encryption and decryption algorithms.

Thus, significant research tasks center around the SDN design to build and present a legitimately unified guide of the system. The up and coming age of SDN systems will profit from the effortlessness of the execution, yet in addition from the way that keeping up and refreshing applications will be simpler too. In this study, we have studied a wide scope of later and best in class extends in SDN.

Our objective was to exhibit these difficulties and present current institutionalization endeavors. In no way, shape or form have we displayed a comprehensive rundown of chances? We accept extra difficulties and open doors for research exists along a wide range extending from SDN arrangements utilized in united bundle and circuit changed systems to formal displaying and model checking to improve the dependability of the SDN-based arrangements.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

Aside from the exploration themes referenced above, there is additionally an examination heading that has not pulled in much consideration, which is the security of SDN. In the event that the security of SDN can't be guaranteed, their improvement will experience a great deal of opposition during the way toward supplanting conventional system engineering and even turned out to be by and large insignificant. In the previous couple of years, so as to address security dangers of SDN, related working associations have been established to think about the comparing security difficulties and arrangements.

At the same time, some solutions against SDN security threats have been proposed, which include controller replication schemes, authentication and authorization mechanisms, schemes to protect controllers against Denial of Service or Distributed Denial of Service (DoS/DDoS) attacks, traffic monitoring and analysis, flow-table overflow attack protection, and others

The Proposed Framework

The module is traditionally responsible for receiving crisp numeric measurements from the environment as input, process them and map them into membership function values. The engine is responsible for processing all calculated membership function values using sets' calculations and communicates with rule base to identify the most suitable output.

 Let **X** be a classical set of objects, called the universe, the elements in **X** are denoted as **x: X = {x}.**

 A set, **A**, in **X**, is characterized by a membership function **μA(x)** that associates each element in **X** with a real number in the unit interval [0, 1].

 The set can be denoted by the set of pairs, **A = {(x, μA(x)), x ε X, μA(x) ε [0, 1]}.**

 μA(x) = 0, implies that **x** does not belong to **A**.

 μA(x) = 1, implies that **x** absolutely belong to **A**.

 When X is a definite set, **{x1 , x2 , …., xn}**, the set A can be represented as **(μA(x1), μA(x2), …, μA(xn)).**

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

The sets and membership functions can be represented in many mathematical forms. However, most of these forms are suitable for decision and control situations in engineering especially in the fields of computer control of machines and robots. In these situations, very sensitive sensors are used to measure different state variables of the machine in a digital or numeric fashion. However, in assessing various situations, it is people who provide assessment of the situation using natural and related terms.

Let $\mathbf{G = \{g_1, g_2 \ldots g_d\}}$ represents the set of assessment grades of an aspect of the model or the organization situation which are in fact a group of sets; namely, **G = {Very High, High, Medium, Low, Very Low}**, and let the sub-measures of that aspect given as; $\mathbf{M = \{m_1, m_2, \ldots m_n\}}$**.** The sub-measures are mapped (fuzzified) into the different grades using the matrix shown below in Figure, where $\boldsymbol{\mu_{ij}} \in [\mathbf{0, 1}]$ and represents the membership value of sub-measure $\mathbf{m_i}$ into the set (grade) $\mathbf{g_j}$.

As it is unnatural for humans to translate their subjective evaluation of each sub-measure into a numeric value, and to accurately capture the human evaluation and judgment, each sub-measure $\mathbf{m_i}$ is assumed to take a value from the set of values **{Very Low, Better Than Very Low, Low, Better Than Low, Medium, Better Than Medium, High, Better Than High, Less Than Very High, Very High}.** This scale represents 10 different levels. Hence, it helps greatly to model the human thinking and assessment process. However, the scale would still need to be translated into numeric values for all $\boldsymbol{\mu_{ij}}$'s. It is impractical if not impossible for humans to translate their subjective evaluation of each sub-measure into numeric values for each membership function representing a grade.

CONCLUSION

Existence of sufficient control over the movement pattern of the mobile platforms in Airborne Networks opens the avenue for designing topologically stable hybrid networks. In this study, we discussed the system model and architecture for Airborne Networks (AN). We studied the problem of maintaining the connectivity in the

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

underlying dynamic graphs of airborne networks with control over the mobility parameters and developed an algorithm to solve the problem.

Unauthorized network access by an outside hacker or a disgruntled employee can cause damage or destruction to proprietary data, negatively affect company productivity, and impede the capability to compete Unauthorized network access can also harm relationships with customers and business partners, who might question the capability of a company to protect its confidential information.

REFERENCES:

Damien Octeau et al., Android Application Software, Journal Of Computer Science, vol. 12, Issue 34, pp. 2345-4366, 2012.

M. Stoces et al., Spatial Data Monitoring and Mobile Applications - Comparison of Methods for Parsing JSON in Android Operating System, Agris on-line Studys in Economics and Informatics, vol. 6, Issue 12, pp. 23-34, 2014.

Sneha. R. Kaware, The Android - A Widely Growing Mobile Operating System With its Mobile based Applications, International Journal of Computer Science and Mobile Applications, Vol. 3, Issue 1, pg. 39-45, 2015.

G. Liu and H. B. Zhang, "Voice Assistant - Application of Speech Recognition Technology in the Android System", Applied Mechanics and Materials, Vol. 596, pp. 384-387, 2014.

X. L. Li and G. X. Lou, "Research and Implementation of Character Recognition System Based on Android Platform", Applied Mechanics and Materials, Vols. 556-562, pp. 4811-4814, 2014.

Robert Goffeney et al., Development Techniques for Android Platform Mobile Device Application, International Journal of Computer Science, vol. 22, Issue 1, pp. 34-45, 2011.

Hayoung Noh, Starting Mobile Application Development for E-Sports Portal, International Conference on Pervasive Technologies Related to Assistive Environments, vol. 2, Issue 14, pp. 254-346, 2010.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 09
September 2022

Pranjal Prateek, Let the Whistle Blow Loud and Clear: Need for Greater Transparency and Certainty in the Leniency Programme, vol. 6, Issue 12, pp. 346-467, 2010.

Bertini, E., et al., Appropriating Heuristic Evaluation for Mobile Computing International Journal of Mobile Human Computer Interaction (IJMHCI), vol. 1, Issue 1, p. 20-41,2009.

Carneiro, G., J. Ruela and M. Ricardo Cross-Layer Design in 4G Wireless Terminals." IEEE Wireless Communications, vol. 11, Issue 2, pp. 7-13, 2014.

Bruns, E. and O. Bimber, Adaptive training of video sets for image recognition on mobile phones. Personal Ubiquitous Comput., vol. 13, Issue 2, p. 165-178, 2010.

Received: *11 August 2022*
Revised: *12 September 2022*
Final Accepted for publication: *14 September 2022*