IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

Securing Mobile Computing: Ensuring Safety in the Digital Realm

Daniya Iqbal Bharoon[1], Sandilkar Saniya Imran[2], Potdar Amey Achyut[3]
Assistant Professor, Department of Computer Science[1]
Student, Department of Computer Science[2,3]
Anjuman Islam Janjira Degree College of Science, Murud-Janjira, Raigad, Maharashtra, India

Abstract: *As more and more people enjoy the various services brought by mobile computing, it is becoming a global trend in today's world. At the same time, securing mobile computing has been paid increasing attention. In this article, we discuss the security issues in mobile computing environment. Reanalyse the security risks confronted by mobile computing and present the existing security mechanisms. As mobile computing becomes increasingly ubiquitous in both personal and professional spheres, ensuring the security of mobile devices and the data they handle is paramount. This paper explores the challenges and solutions involved in securing mobile computing environments to maintain confidentiality, integrity, and availability. The abstract begins by examining the unique characteristics of mobile computing, including limited resources, diverse communication channels, and varying degrees of trust in network infrastructures. These characteristics introduce vulnerabilities that must be addressed to mitigate risks effectively. Next, the paper discusses the fundamental principles of mobile security, including encryption, authentication, and access control. These principles form the basis of a comprehensive security framework designed to protect data both at rest and in transit. Techniques such as end-to-end encryption, biometric authentication, and multi-factor authentication are explored in detail.*

Keywords: mobile computing

I. INTRODUCTION

Mobile computing has become an integral part of modern life, revolutionizing the way we work, communicate, and access information. The pervasive adoption of smartphones, tablets, and other mobile devices has empowered individuals and organizations with unprecedented convenience and flexibility, enabling anytime, anywhere access to a wealth of resources and services. However, this paradigm shift towards mobile-centric computing has also brought about a myriad of security challenges, as the boundary between personal and professional use blurs, and sensitive data travers's diverse networks and endpoints.

In this rapidly evolving landscape, the security of mobile devices and the data they handle has emerged as a critical concern for individuals, businesses, and governments alike. The inherent characteristics of mobile computing, including limited resources, heterogeneous environments, and ubiquitous connectivity, introduce unique vulnerabilities that adversaries are quick to exploit. From unauthorized access to data breaches and malware attacks, the risks associated with mobile computing are diverse and constantly evolving, necessitating a proactive and multifaceted approach to security.

This paper seeks to explore the complexities of securing mobile computing environments, with a focus on preserving the confidentiality, integrity, and availability of data and systems. By examining the fundamental principles of mobile security, the challenges posed by emerging threats, and the innovative solutions and technologies available, this paper aims to provide a comprehensive understanding of the strategies and best practices essential for safeguarding mobile assets in an increasingly interconnected world.

II. MOBILE COMPUTING AT A GLANCE

Mobile computing represents a revolution in how we engage with technology, offering the freedom to access information and services from virtually anywhere, at any time. This paradigm shift is underpinned by ubiquitous

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

connectivity, with mobile devices leveraging wireless networks like Wi-Fi and cellular data to stay connected on the go. Unlike traditional computing devices confined to fixed locations, mobile devices are designed for portability, empowering users to remain productive while traveling, commuting, or working remotely. With a diverse array of form factors including smartphones, tablets, and wearables, mobile computing caters to a wide range of preferences and use cases. Central to the mobile experience is the rich ecosystem of apps, which provide access to services spanning social media, productivity tools, entertainment, and beyond. These apps are easily discoverable and installable through app stores, enhancing the functionality and versatility of mobile devices.

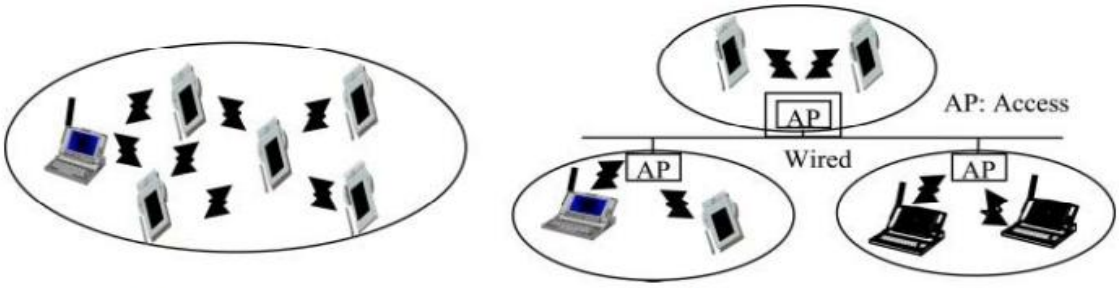
Wireless local area networks (WLANs) have gained enhanced usefulness and acceptability by providing a wider coverage range and an increased transfer rate. The most well-known representatives of WLANs are based on the standards IEEE 802.11[1], HiperLAN and their variants. IEEE 802.11 has been the predominant standard for WLANs, which support two types of WLAN architectures by offering two modes of operation, ad-hoc mode and client-server mode. In ad-hoc (also known as peer-to-peer) mode (Figure 1(a)), connections between two or more devices are established in an instantaneous manner without the support of a central controller. The client-server mode (Figure 1(b)) is chosen in architectures where individual network devices connect to the wired network via a dedicated infrastructure (known as access point), which serves as a bridge between the mobile devices and the wired network. This type of connection is comparable to a centralized LAN architecture with servers offering services and clients accessing them. A larger area can be covered by installing several access points, as with cellular structure having overlapped access areas.

III. WHY IS SECURITY AN ISSUE?

Security is a prerequisite for every network, but mobile computing presents more security issues than traditional networks due to the additional constraints imposed by the characteristics of wireless transmission and the demand for mobility and portability. We address the security problems for both infrastructure-based WLANs and infrastructure-less ad hoc networks.

3.1 Security Risks of Infrastructure-Based WLANs

Because a wireless LAN signal is not limited to the physical boundary of a building, potential exists for unauthorized access to the network from personnel outside the intended coverage area. Most security concerns arise from this aspect of a WLANs and fall into the following basic categories:



(a) Infrastructure-less (b) Infrastructure-based Network

Fig. 1. WLAN Architectures

- **Limited Physical Security.** Unlike traditional LANs, which require a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point (AP) device. As shown in Figure 1 an access point communicates with devices equipped with wireless network adaptors and connects to a fixed network infrastructure.
- **Constrained Network Bandwidth.** The use of wireless communication typically implies a lower bandwidth than that of traditional wired networks. This may limit the number and size of the message transmitted during protocol execution. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency,

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

corrupting the signal until the network ceases to function. Since the aim of this type of attack is to disable accessing network service from the legitimate network users, they are often named denial of service (DoS) attack. Denial of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

- **Energy Constrained Mobile Hosts.** To support mobility and portability, mobile devices generally obtain their energy through batteries or other exhaustive means, hence they are considered as energy constrained mobile hosts. Energy Constrained Mobile Hosts. To support mobility and portability, mobile devices generally obtain their energy through batteries or other exhaustive means, hence they are considered as energy constrained mobile hosts.

3.2 More Vulnerabilities of Infrastructure-Less Ad Hoc Networks

In ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are roaming independently and are able to move freely with an arbitrary speed and direction. Thus, the topology of the network may change randomly and frequently. In such a network, the information transfer is implemented in a multi-hop fashion, i.e., each node acts not only as a host, but also as a router, forwarding packets for those nodes that are not in direct transmission range with each other. By nature, an ad hoc network is a highly dynamic self-organizing network with scarce channels. Besides these security risks, ad hoc networks are prone to more security threats due to their difference from conventional infrastructure-based wireless networks.

- **The Lack of Pre-fixed Infrastructure** means there is no centralized control for the network services. The network functions by cooperative participation of all nodes in a distributed fashion. The decentralized decision making is prone to the attacks that are designed to break the cooperative algorithms. A malicious user could simply block or modify the traffic traversing it by refusing to cooperate and break the cooperative algorithms.
- **Dynamically Changing Topology** aids the attackers to update routing information maliciously by pretending this to be legitimate topological change. Any intruder can maliciously give incorrect updating information. For instance, DoS attack can be easily launched if a malicious node floods the network with spurious routing messages. The other nodes may unknowingly propagate the messages.
- **Energy Consumption Attack** is more serious as each mobile node also forwards packets for other nodes. An attacker can easily send some old messages to a node, aiming to overload the network and deplete the node's resources. More seriously, an attack can create a rushing attack by sending many routing request packets with high frequency, in an attempt to keep other nodes busy with the route discovery process, so the network service cannot be achieved by other legitimate nodes.
- **Node Selfishness** is a specific security issue to ad hoc network. Since routing and network management are carried by all available nodes in ad hoc networks, some nodes may selfishly deny the routing request from other nodes to save their own resources (e.g., battery power, memory, CPU).

IV. SECURITY COUNTERMEASURES

Secure mobile computing is critical in the development of any application of wireless networks.

Security Requirements

Similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation.

- **Availability** ensures that the intended network services are available to the intended parties when needed.
- **Confidentiality** ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.
- **Authenticity** allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

- **Integrity guarantees** that information is never corrupted during transmission. Only the authorized parties are able to modify it.
- **Non-repudiation** ensures that an entity can prove the transmission or reception of information by another entity, i.e., a sender/receiver cannot falsely deny having received or sent certain data.

WLAN Basic Security Mechanisms

The IEEE 802.11b standard identifies several security services such as encryption and authentication to provide a secure operating environment and to make the wireless traffic as secure as wired traffic. In the IEEE 802.11b standard, these services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link level data during wireless transmission between clients and APs. That is, WEP does not provide any end-to-end security but only for the wireless portion of the connection. A part from WEP, other well-known methods that are built into 802.11b networks are: Service Set Identifier (SSID), Media Access Control (MAC) address filtering, and open system or shared-key authentication.

- **SSID.** Network access control can be implemented using an SSID associated with an AP or group of APs. Each AP is programmed with an SSID corresponding to a specific wireless LAN. To access this network, client computers must be configured with the correct SSID. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations. Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the AP is configured to broadcast its SSID.
- **MAC Address Filtering.** While an AP can be identified by an SSID, a client computer can be identified by a unique MAC address of its 802.11b network card. To increase the security of an 802.11b network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client is not allowed to associate with the AP.

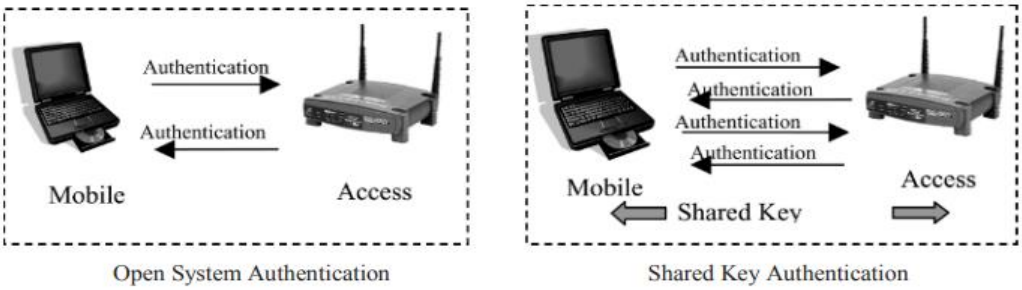


Fig. 2. IEEE 802.11 Authentication Modes

- **Authentication.** In a WLAN, an AP must authenticate a client before the client can associate with the AP or communicate with the network. The IEEE 802.11b standard has defined two types of authentication methods: open system and shared Key. Open system authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the any SSID option to associate with any available AP within range, regardless of its SSID. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. Figure 2 illustrates the two authentication modes. By default, IEEE 802.11b wireless devices operate in an open system authentication mode. Both of these authentication modes are one-way authentication, i.e., the mobile clients can be authenticated by the APs, but the authenticity of APs is not authenticated. Thereby, a rogue node may masquerade as an AP and establish communication with the mobile nodes.
- **WEP-Based Security.** WEP security protocol encrypts the communication between the client and an AP. It employs the symmetric key encryption algorithm, RC4 Pseudo Random Number Generator. Under WEP, all clients and APs on a wireless network typically use the same key to encrypt and decrypt data. The key resides

Copyright to IJARSCT
www.ijarsct.co.in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

in the client computer and in each AP on the network. The 802.11b standard does not specify a key-management protocol, so all WEP keys on a network usually must be managed manually and are static for a long period of time. This is a well-known security vulnerability. Support for WEP is standard on most current 802.11 cards and APs. WEP specifies the use of a 40-bit encryption key. The encryption key is concatenated with a 24-bit initialization vector (IV), resulting in a 64-bit key. This key is input into a pseudorandom number generator.

It is clear that this traditional WLAN security that relies on SSIDs, open system or shared key authentication, MAC address filtering, and static WEP keys is better than no security at all, but it is insufficient, and a new security solution is needed to secure mobile computing.

Advanced WLAN Security Mechanisms

- **WEP2.** As an interim improved solution to the many flaws of WEP, the TGI Working Group of the IEEE proposed WEP2. Unfortunately, similar to major problems with WEP, WEP2 is not an ideal solution. The main improvement of WEP2 is to increase the IV key space to 128 bits, but it fails to prevent IV replay and still permits IV key reuse. The weakness of plaintext exploits and same IV replay are the same with that in WEP. In WEP2, the authentication is still a one-way authentication mode, and the problem of rogue AP is not solved.
- **Virtual Private Networking (VPN).** To further address the concerns with WEP security, many organizations adopt the virtual private network (VPN) technology. The VPN approach has a number of advantages. Firstly, it is scalable to a large number of 802.11 clients and has low administration requirements for the IEEE 802.11 APs and clients. Secondly, the VPN servers can be centrally administered and the traffic to the internal network is isolated until VPN authentication is performed. Thirdly, if this approach is deployed then a WEP key and MAC address list management is not needed because of security measures created by the VPN channel itself. This is a good solution for networks, particularly with existing VPN infrastructure for remote access.

V. ADDITIONAL SECURITY REQUIREMENTS OF AD HOC NETWORKS

As ad hoc networking is somewhat different from the traditional approaches, designing an efficient security scheme to protect ad hoc networks is confronted with several new requirements.

First, the key management mechanism should be implemented in a distributed fashion. Ad hoc network is a distributed network, in which network connectivity and network services, for example, routing, are maintained by the nodes themselves within the network. Each node has an equal functionality. There are no dedicated service nodes, which can work as a trusted authority to generate and distribute the network keys or provide certificates to the nodes, as the certificate authority (CA) does in the traditional public key infrastructure (PKI) supported approaches. Even if the service node can be defined, keeping the availability of the service node to all the nodes in such a dynamic network is not an easy task.

Secondly, light-weight authentication and encryption scheme with resource awareness are required. The low resource availability necessitates their efficient utilization and prevents the use of complex authentication and encryption algorithms. Public-key cryptography-based authentication and encryption mechanisms are fully developed in securing traditional networks. Unfortunately, generation and verification of digital signatures are relatively expensive, which limits its acceptance to ad hoc networks. Symmetric cryptography is more efficient than public-key based asymmetric primitives due to its moderate resource consumption, but it requires both the sender and receiver to share a secret. In ad hoc networks, the problem is how to distribute the shared keys safely so that only the two parties (correct sender and receiver) would get it and not anyone else. It is thus challenging to define some new efficient cryptography algorithms for designing a light-weight authentication and encryption scheme.

Thirdly, combination of intrusion prevention and intrusion detection mechanisms is necessary. The work on securing wireless ad hoc networks can be classified into two types, intrusion prevention and intrusion detection. Intrusion prevention implies developing secured protocols or modifying the logic of existing protocols to make them secure. Most of the key based security protocols belong to this type. The idea of intrusion detection is to characterize the user

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

normal behaviour within the network in terms of a set of relevant system features. Once the set of system features is selected, the classification model is built to detect the anomalies from its normal behaviour. Currently, the research on intrusion prevention and intrusion detection is done separately, and intrusion prevention has been paid more attention. But actually, they are not independent of each other, and should work together to provide security services. For example, intrusion prevention approaches can efficiently deal with the attacks coming from the outsiders by constraining the network access control, but it has no way to handle the denial-of-service attacks performed by the compromised nodes who have all the keys to access the network. Indeed, some active attacks can be efficiently detected because of a large deviation of attackers' behaviour from the normal user behaviour. Therefore, a security scheme combining these two mechanisms is suitable to better secure ad hoc networks.

VI. SECURITY SCHEMES FOR AD HOC NETWORKS

In the recent research of security in wireless ad hoc networks, several good security approaches have been proposed, and they generally fall into three categories, secure routing, trust and key management, and service availability protection.

Secure Routing

The process of implementing and enforcing security measures within network routing protocols to ensure that data transmission across a network is reliable, confidential, and tamper-proof. This involves the authentication of routing paths, protection of the integrity and privacy of data, and maintaining the availability of the network against attacks.
Secure routing aims to counter threats that compromise the integrity of data, the authenticity of routing paths, and the overall security of network operations. It includes a combination of cryptographic techniques, secure protocols, and policy enforcement measures designed to safeguard the routing infrastructure and the data it carries.

Trust and Key Management

Most of the protocols discussed above make an assumption that efficient key distribution and management has been implemented by some kind of key distribution centre, or by a certificate authority, which has super power to keep connecting to the network and cannot be compromised, but how to maintain the server safely and keep it available when needed presents another major issue and cannot be easily solved. The problem of this solution is that it still requires an administrative infrastructure available to distribute the shares to the special nodes and issue the public/private key pairs to all the nodes. How to keep the n special nodes available when needed and how the normal nodes know how to locate the server nodes make the system maintenance difficult. In Kong et al. proposed another threshold cryptography scheme by distributing the RSA certificate signing key to all the nodes in the network. This scheme can be considered as having a fully distributed certificate authority, in which the capabilities of certificate authority are distributed to all nodes and any operations requiring the certificate authority's private key can only be performed by a coalition of k or more nodes. This solution is better in the sense that it is easier for a node to locate k neighbour nodes and request the certificate authority service since all nodes are part of the certificate authority service, but it requires a set of complex maintenance protocols.

VII. METHODOLOGY

Implementing secure mobile computing requires a comprehensive approach that encompasses several key areas to protect data, maintain privacy, and ensure device integrity. First, device security is critical and can be addressed by enforcing strong access controls such as passwords, PINs, or biometric systems, and by using encryption to secure data at rest. Devices should also support and enable secure boot processes that verify only trusted software is loaded during startup. Application security is another vital aspect, involving the management of app permissions to limit access only to essential functions and data, encouraging the installation of applications from trusted sources, and keeping all applications up-to-date to safeguard against vulnerabilities.
Network security is equally important; it involves using virtual private networks (VPNs) to encrypt data over unsecured networks, installing mobile-specific firewalls, and educating users about the dangers of public Wi-Fi. Regarding data security, practices like data minimization and regular backups to encrypted cloud storage or secure locations are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

recommended to avoid data loss and protect sensitive information. Educating users plays a crucial role in mobile security, encompassing regular training on security threats, safe practices, and the importance of updates.

VIII. REVIEW OF LITERATURE

A review of literature on secure mobile computing necessitates a comprehensive examination of existing studies, covering various aspects crucial to understanding and improving the security of mobile devices and their applications. The focus areas typically include device security, which delves into encryption methods, biometric implementations, and secure boot processes to ensure data integrity and prevent unauthorized access. Application security is another critical area, where research often explores secure coding practices, the security measures of application stores, and the effectiveness of app management strategies. Network security is equally important, with literature examining the robustness of VPNs, the security challenges posed by public Wi-Fi, and the effectiveness of different network protocols in safeguarding data transmission.

Additionally, user behaviour and education emerge as significant themes, highlighting the effectiveness of security training and identifying common pitfalls in user interactions with mobile technology. Policies and compliance, particularly regarding mobile device management and adherence to international standards, also form a substantial part of the literature, reflecting the legal and regulatory dimensions of mobile computing. Emerging technologies such as the use of AI for threat detection and blockchain for enhancing data integrity are frequently discussed, pointing to new directions in mobile security solutions.

IX. RESULT AND DISCUSSION

In the "Results" section of a study on secure mobile computing, the findings are systematically presented without interpretation. This might include quantitative data on the effectiveness of encryption algorithms or qualitative insights from user surveys regarding mobile security practices. The section employs clear and concise language, often supplemented with tables, graphs, or figures to illustrate the results effectively. Statistical analysis is detailed enough to support conclusions but remains accessible to readers with varying levels of statistical expertise. Meanwhile, in the "Discussion" section, the results are interpreted within the broader context of mobile computing security. Findings are contextualized within existing research, anomalies are explained, and practical implications are explored. Any limitations of the study are acknowledged, and suggestions for future research are proposed, highlighting theoretical advancements and practical applications. Ultimately, the integration of results and discussion contributes to a cohesive narrative that demonstrates the value of the research and its impact on advancing secure mobile computing practices.

X. CONCLUSION

Mobile computing technology provides anytime and anywhere service to mobile users by combining wireless networking and mobility, which would engender various new applications and services. However, the inherent characteristics of wireless communication and the demand for mobility and portability make mobile computing more vulnerable to various threats than traditional networks. Securing mobile computing is critical to develop viable applications. In this article, we discussed the security issues faced by mobile computing technology. We analysed the various security threats and describe the existing current countermeasures. We have seen that many security solutions have been proposed to securing WLANs, but no one is able to claim that it solves all the security problems, or even most of them. In essence, secure mobile computing would be a long-term ongoing research topic.

XI. ACKNOWLEDGEMENT

In the acknowledgment section of our research on secure mobile computing, we extend our gratitude to several individuals and organizations whose support and contributions were invaluable throughout this endeavour. First and foremost, we express our sincere appreciation to our supervisors and advisors for their guidance, encouragement, and expertise, which significantly influenced the direction and quality of our research. We also acknowledge the generous financial support provided by without which this study would not have been possible. Furthermore, we are grateful to our collaborators and colleagues who contributed their time, knowledge, and assistance during various stages of the research project. Special thanks are extended to the participants who volunteered their time and insights, enabling us to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, May 2024

gather valuable data and insights. Additionally, we acknowledge the support and resources provided by including access to facilities and equipment essential for conducting our research. We also appreciate the support of our friends and family members who provided encouragement and understanding throughout the research process. Lastly, we thank the professional editors or proofreaders who assisted with refining the manuscript. Each of these individuals and entities played a crucial role in the completion of this study, and we are deeply grateful for their contributions.

REFERENCES

[1] LAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE Standard 802.11, 1999 Edition, 1999.

[2] D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole publisher, 2002. [3] J. Walker, overview of IEEE 802.11b Security, http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.

[4] N. Borisov, I. Goldberg, and D. Wagner, intercepting Mobile Communications: The Insecurity of 802.11î, http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields, A Secure Routing Protocol for Ad Hoc Networks, I Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[6] M. G. Zapata, secure Ad hoc On-Demand Distance Vector Routing, I ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 6 , No. 3, pp. 106-107, 2002.

[7] Y. C. Hu and D. B. Johnson and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks, I Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13, 2002.

[8] Y. C. Hu, A. Perrig, and D. B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, I Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, September, 2002.

[9] Perrig, R. Canetti, B. Whillock, "TESLA: Multicast Source Authentication Transform Specification", http://www.ietf.org/internet-drafts/draft-ietf-msectesla-spec-00.txt, October 2002.

[10] L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad hoc Networks," JPDC Special Issue on Mobile Ad Hoc Networking and Computing, Vol. 63, No. 2, Feb. 2003, pp. 214-227