A Brief Assessment of Mobile Security, Vulnerabilities and Threats

Aakanksha[1], Ahana Jha[2], Anam[3*]

ABSTRACT

With the advent of increasingly convenient technology that can be utilized through a smartphone, handheld devices such as phones and tablets have practically become a necessity. The rising necessity of a phone for every mundane task to be carried out in everyday life has made it such that an alarming amount of the user's personal information is stored on their handheld devices. It is not uncommon for children as young as 12 to possess such devices, and be completely proficient in using them. These conveniences, however, do not come free of cost—in most cases, the cost is the user's privacy. This paper is aimed at analysing the existing work done about phone hacking to identify the major threats to user privacy, and present this information in a cohesive manner for perusal. To this end, the paper is divided into 2 sub topics. It gives succinct overviews of the identified threats and vulnerabilities that facilitate phone hacking and exploitation of user's privacy. Overall, through this paper, we hope to incite increased risk awareness surrounding mobile devices and their associated vulnerabilities and security threats.

Keywords : *Mobile Security, Phone Hacking, Mobile Threats.*

1. Introduction

As the use of technology evolves and the usage of mobile devices becomes increasingly common and integral to everyday life, the possibilities of crime and exploitation via this avenue also increase. Hacking into a personal mobile device has become concerningly lucrative in regards to both the quality and quantity of user data that can be gained. This paper is aimed at exploring and reviewing existing data and literature surrounding phone hacking, and identifying the major threats and exploitable vulnerabilities in user devices. We divide the paper into two sections – the first section gives an overview of what 'phone hacking' entails – the methods used to accomplish it, as well as the harm it can cause. It explores four avenues used for hacking by reviewing literature written to outline the methods of hacking over Bluetooth, using malware, keylogger software and camera-based hacking. The second section explores in brief common security threats targeted at mobile devices. Through this paper, we hope to incite increased risk awareness surrounding mobile devices and their associated vulnerabilities and security threats. This study aims to accomplish this by reviewing and exploring previously compiled literature on the relevant topics.

2. Literature Review

The study conducted by Khan et al. (2015), examined the risks, weaknesses, and security issues that exist in mobile ecosystems. It highlights how crucial it is to safeguard user privacy regarding data from a range of mobile security risks. The writers go over defence tactics to protect private and corporate information, such as biometric authentication. The usefulness of biometric techniques is highlighted through a comparison study of various security measures.

Dahiya et al. (2024) talked about the value of mobile devices in everyday life as well as the security threats they pose. It highlights how important it is to safeguard user information and uphold client confidence. Data leaks, malware assaults, network congestion, lack of standardization, and new technologies like 5G and IoT are some of the major issues. Other major problems are user behaviour and regulatory compliance. To address the issues, the study recommends encryption, network segmentation, multi-factor authentication, user education, frequent upgrades and investment in security measures.

Storing massive amounts of data is made efficient with cloud-based data warehousing. It assists in meeting user requirements for data security. The research study by Ahmadi (2023) covered the challenges associated with cloud-based data warehousing security and privacy, stressing potential threats such as privacy concerns, malware attacks, and data breaches. It highlights how crucial cloud data warehousing is to the scalability and

1. *Department of Computer Science, Shaheed Rajguru College, University of Delhi.*
2. *Department of Computer Science, Shaheed Rajguru College, University of Delhi.*
3. *Department of Computer Science, Shaheed Rajguru College, University of Delhi.*
* *Corresponding Author ✉ anamm0385@gmail.com*

Received: 20 September, 2024
Available online: 25 October, 2024

affordability of contemporary IT infrastructure. The study examines previous research on privacy issues, security issues, and regulatory compliance. It makes recommendations for data protection strategies, including data masking, encryption, and compliance with privacy laws.

The convenience of mobile payments (MP) has led to their widespread popularity. Furthermore, a single mobile device can have several services easily linked into it thanks to Near Field Communication (NFC) technology. The research study by Shahad & Al-Hajia (2024) offers a thorough analysis of the security environment for Secure Mobile Payment (SMP) systems, emphasizing the difficulties and possible solutions. It talks about how Near Field Communication (NFC) technology affects mobile payment systems and how different services can be combined into one mobile device. The paper examines the benefits, drawbacks, and technological aspects of SMP, including biometric identification, tokenization, and encryption. It also looks at the limitations of SMP's widespread application as well as how it affects financial transactions. In order to ensure a reliable payment ecosystem, the paper seeks to advance awareness of and use of safe digital transactions.

Android devices have long been vulnerable to overlay attacks, which pose a serious security risk. A technique for identifying overlay attacks on Android devices is covered in the study by Kar et al. (2024). It explains how content can be shown over other programs using overlays, raising security issues. In order to improve Android device security by detecting vulnerabilities and safeguarding user privacy and data security, it suggests a detection method that combines static detection and activity behaviour analysis.

3. Phone Hacking : Common Threats

Phone hacking refers to exploration and/or exploitation of vulnerabilities in the security framework of mobile phones in specific. Because of their portability and increasing utility, the amount of information one can gain by hacking into a victim's phone has become damningly encompassing. If a person's phone is compromised, it means that the attacker has gained enough information to damage not only the victim, but people and organizations associated with the victim as well. Studies have found that mobile devices pose a risk to organizations when used and transported outside physical boundaries, and can facilitate espionage and theft (Kar et al., 2024).

Phones are vulnerable in alarmingly numerous ways, and some prominent methods of hacking that exploit these vulnerabilities are listed below:

3.1 Bluetooth

Bluetooth has become an increasingly prevalent way of communication and connection, and provides a convenient avenue for information exchange without the use of internet. Bluetooth connections can be either Classical Bluetooth – the original version, used for the sharing of large data such as media files – or Bluetooth Low Energy – a newer version designed for low-power devices like smartphones (Muraleedhara et al., 2024).

There are three modes of security employed in this technology :

- Security Mode 1- Provides no security enforcement.
- Security Mode 2 - Service level security enforcement.
- Security Mode 3 - Highest level of security enforcement.

There is a default level of security in all Bluetooth devices, and within this there exist 3 levels of security: the requirement of authentication and authorization, of authentication only, or neither in order to avail a service. Bluetooth devices also employ 2 levels of security in regards to other devices, and categorize them as either trusted or untrusted devices (Browning & Kessler, 2009).

As per the study by Muraleedhara et al. (2024), the most common Bluetooth vulnerability exploits include:

- *Bluesnarfing* : Attackers can gain unauthorized access by exploiting a firmware flaw in older devices (circa 2003).
- *Bluejacking* : In this, the attackers spam the Bluetooth enabled device with unsolicited phishing messages. This attack has a range of 10 m for mobile phones, and 100 m for laptops. Although data is not directly being stolen in this attack, it opens the device to further invasions and puts the user privacy at risk all the same. Further, it can be used for harassment by sending abusive messages.
- *Bluebugging* : This attack allows the hacker to gain access to Bluetooth enabled devices and its commands by exploiting a firmware security flaw of older devices (circa 2004), provided the attacker is within close range of the target device. In this, the attacker will try and gain access to the device, and then usually install a backdoor that allows them to access the device again and launch further attacks.
- *Bluesmacking* : This is a Denial of Service (DoS) attack that is aimed at overwhelming the capacity of the target device and forcing it to shut down.
- *Car whispering* : This method exploits the unchanged default passkey set in an automobile's hands-free Bluetooth audio kits, and allows the attacker to transmit audio to the car's speaker kit and eavesdrop using its microphone.

3.2 Malware

Malware is any malicious software that seeks to exploit the vulnerabilities in the victim's system for personal gain for the attacker. Malware, though initially targeted towards PCs, has over time evolved to attack mobile devices and

specially phones as well. 'Cabir' was the first mobile malware, and targeted Symbian-based platforms. Due to the enormous amount of personal information that can be accessed via mobile phones, mobile malware has become increasingly prominent and with it, the loss caused by them as well (Moses & Morris, 2021).

There are many methods of infection that might help propagate the malware.

- **Bluetooth/SMS distribution :** Bluetooth technology is used to share multimedia files between connected devices, and is embedded into most devices. It has become more precise and advanced over time, and is a very important and versatile means of information exchange. However, it is also a prominent method of malware propagation for these very reasons as well. This method has a large threshold of infection; unlike Wi-Fi propagation, it is not limited by user's data balance.

  Propagation via SMS or MMS entails the distribution of payload by sending unauthorized texts from victim's device, thus incurring SMS/MMS costs for the victim and infecting the recipient.
- **USB/network distribution :** In this method, when a mobile device is connected via USB to an infected PC, the malware is transmitted over the connection onto the phone. When a connection between a mobile device and the USB is established, a malware with access to the relevant ports and cables will infect the connected device, if the USB has the product model 2071, 02A or 10A, as stated by the IBM.
- **Market to device distribution :** The propagation mechanism of Application to Device (A2D) depends on application vulnerability for the distribution of malware. Market to Device approach depends on the user's decision to install a malicious application that has been uploaded onto the app market and disguised as something benign. This type of propagation is dependent on the market response to the carrier application.

Major attack goals for mobile malware include sabotage, fraud, data theft, spam and misuse of service, to the ends of financial profit, ID theft, personal information theft, and industrial espionage. The study by Moses & Morris (2021) examines six malware variants, which are briefly discussed in this sub-section :

1. Ransomware

Ransomware are designed to block access to a device or data, typically by encrypting files, until a demanded amount of money is paid, typically in bitcoin. While unusual for mobile phones to be attacked using this method, nevertheless, in recent times, studies show that 74% of companies are besieged by ransomware attacks.

2. Trojan

Trojans are used to harvest sensitive data from a device, and are planted by being disguised as a harmless and legitimate application. The paper notes that android trojans have a tendency to be disguised as legitimate banking applications, and harvest user's credentials. Some android trojans include :

- *Unnamed trojan '888.apk'* : intercepts and sniffs mobile banking transaction packets during SMS alerts and transaction commands.
- *Trojan-SMS.AndroidOS.Svpeng* : steals mobile banking credentials upon the launch of a banking application.

3. Adware

This type of malicious program was initially only known for being frustrating with the constant pop-ups on screen. It has since then progressed to being used for data collection purposes as well, even performing jailbreaking and rooting on mobile phones. They can employ social engineering tactics to obtain sensitive data from victims. An example of adware is Cydia, which steals user data.

4. Rootkit

This is a type of malware that uses remote access to exploit a compromised device. A rootkit has three components – loader, rootkit, dropper. It gains administrative privileges and alters configurations of a device, allowing it to install other malicious software into the device without the user's consent. It is a very difficult malware to remove, since it is both silent and subtle in its working. An example of a rootkit is HummingBad, which steals credentials by installing other apps to create fake ads in the background.

5. Botnets and viruses

Botnets are compromised devices, which are being controlled remotely by the attacker, called the 'botmaster'. Botnets are used to launch DDoS attacks, which has made them a serious threat to cybersecurity. An example of a botnet is Double-Door.

Mobile viruses are pieces of malicious code meant to attack devices and propagate itself through the cellular environment of the device. They are propagated when the infected application or file is executed. They can cause data and application lose, and even device destruction.

6. Worms

Worms are pieces of self-replicating malicious code, requiring little to no external trigger. They can assume various file formats. The payload of this kind of malware executes once on the initial device, and then moves to other target devices using TCP, email, etc as attack vectors.

The study classifies worms into five major categories:

- *Binary file worms* : These infect executable files. Usually in machine language for easy payload distribution.
- *Multi-partite worms* : They can infect the boot sector and executable files, although they are rare.

- *Script file worms :* They are written in human readable form, so they need to be translated before being executed as machine code.
- *Binary stream worms:* Infection vector is deployed through network connection, and needs the devices to be linked so it can propagate.
- *Macro worms* : They infect applications and document files. They are the most commonly encountered type of worm.

3.3 Keylogger

Conceptually, keyloggers can be differentiated as Keystroke Loggers – ones that use the process of tracking and recording every key entered by user, and record information such as speed, time, name of the key, and the length of press – and Keylogger Tools – these can be hardware or software that are designed to track and record every keystroke made by user. The information recorded using keyloggers can be used for malicious purposes without the user's knowledge or consent. This information can sometimes even include GPS locations, mic or camera footage, calls, or copy-paste clipboard information. The techniques that can be used to achieve keylogging can vary from hardware manipulation, I/O interception, video surveillance, tampering with keyboard or filter drivers, manipulation of DLL functions, etc (Ruhani & Zolkipli, 2023).

The security threat posed by keylogger software in regards to personal and financial safety is further exacerbated by the notable security gap generated by third party android keyboards' propensity to ask for user permissions (Kuncoro & Kusuma, 2018).

This is a prominent class of malware that harvests sensitive data, and whose implementation aims to avoid detection by security software. Some malicious software can detect the presence of such security measures and avoid them by acting benign and non-malicious.

3.4 Camera-Based

Phone cameras bring with them their own security issues, alongside several new attacks based on the usage of phone cameras. Phone cameras can be used to take photos or recordings without the user's knowledge. Spy camera apps that allow users to take photos and videos of other people without their permission can also prey on the users themselves. Camera permission is one of the most commonly requested permissions, both among harmless and malicious apps (Wu et al., 2014).

With the increasing importance of carrying one's phone everywhere one goes, the amount of private information that is left vulnerable to camera-based attacks can result in serious damages.

However, the role of a spy camera depends on the user's intentions – it can be used to keep an eye on your pets, or to track your phone's location in case of theft or misplacement. On the other hand, the same app performing these benign actions can also be secretly recording personal moments and sending them to a malicious third party.

Some camera-based attacks include :

- **The remote-controlled real-time monitoring attack** - Here the attacker is in complete control over the spy camera app and can launch and record using it at will.
- **The video-based password inference attack** - This attack uses the front camera to track the user's eye movements to deduce what they are typing into the device. Application based, screen unlocking, and video-based eye tracking attacks fall under this umbrella. In the eye tracking field, two types of techniques are used: infrared spectrum imaging and visible spectrum imaging. The former is more accurate, but is not practical as most devices are not equipped with an infrared camera anyways. This kind of attack results in a high possibility of a compromised patterns and PINs as compared to passwords, due to the tight configuration of the keyboards.

The spy camera running and transferring data in the background is not detected by either of two prominent antivirus applications, showing their resistance to detection and security measures and yet again putting into perspective the magnitude of the threat posed (Wu et al., 2014).

3.5 AI Based Threats

With the steadily growing utility of Artificial Intelligence (AI) Systems, it is important to consider the implications this has for cybersecurity. AI technology is vast and is applied in equally vast measures across various fields, some examples of which are search prediction, recommendation feeds on social media, and various generative AI tools, like ChatGPT and Midjourney, which can provide an output based on the input variables on the basis of studying and learning from a database. While AI can be applied to enhance robustness of cybersecurity systems, it cannot be considered a replacement for human minds. It lacks the creativity and intuition of a human adversary. In fact, data poisoning and adversarial attacks can be used to impede the learning process of AI systems – with skewed data to learn from, the predictive ability of the system becomes flawed.

With the powerful processing capacity of AI systems, it is possible for attackers to adapt faster, execute inhumanly high-speed attacks, precisely exploit vulnerabilities, and even mimic human behaviour to enhance the effectiveness of phishing attacks. It can also be used to create malware that is more adaptable and flexible to its environment, and can better escape detection and purging. An example of this is DeepLocker – a highly intelligent malware that can conceal its malintent until it reaches a specific victim, using a combination of AI and

indicators such as facial recognition to identify the target (He et al., 2015).

Moreover, there is the privacy risk that is associated with data collection and usage for the development of AI. A way to mitigate this is by anonymizing user data, and having strict ethical considerations guiding the usage of such data. There are various regulations in place to guide the use of personal data for such purposes, but they are not infallible. Unauthorized access to such data can be devastating (Kumar et al., 2023).

4. Mobile Security Threats

We use smartphones to store hefty amounts of data which operate over WLANs, Bluetooth PANs, and international cellular networks. Smartphones utilise a wide range of sophisticated operating systems, including Windows Mobile, Symbian, iOS, BlackBerry OS, and Android. These machines are more vulnerable than typical PCs due to their extensive network access and rich diversified coding. Smartphones are vulnerable because they frequently retain personal data. Some data can be very sensitive, especially as more and more users conduct financial transactions on their smartphones, like online banking and shopping. Smartphones are lucrative targets for hackers since they may profit significantly from such sensitive data. The Android platform is being used in an increasing number of handsets. The open-source kernel philosophy of Android gives malware authors a better understanding of the mobile platform. To increase market share, Google's marketing strategy encourages the creation of third-party apps and makes releasing them simple. As a result, hackers have lots of opportunities to produce and distribute malware. Additionally, as users develop a habit of downloading and installing apps for their smartphones, the likelihood of malware installation rises. Most customers mistakenly believe that smartphones are simply mobile phones with a selection of communications and entertainment apps pre-installed. They are unaware that their smartphones are essentially portable computers that can be attacked by hackers. As a result, security precautions are not given adequate consideration. The hardware and operating systems of smartphones have made it easier for malware writers to carry out their harmful deeds.

The main concern when a mobile device is lost, stolen, or hacked is data leakage. How to know if your phone has been hacked? If you've noticed anything unusual on your phone like draining of battery more quickly than usual, some mysterious apps running in the background, pop-up ads appearing etc., this may indicate that your devices are compromised. Although these activities don't always mean that your phone is at risk but they could be important signs that your device is compromised. If you discover that your phone is operating much slower than usual, malware might be installed on it. Smartphone performance can deteriorate over time, but it shouldn't happen suddenly. Harmful apps make phone consume more processing power, which will slow down your device. Pop-up advertising may occasionally be expected when browsing the internet, they may also occur on reputable websites or even when you're not expecting them to. Adware may conceal themselves beneath these pop-up advertisements and may harm your phone. More pop-up ads indicate the presence of a virus in the background. Draining of battery more quickly than usual could indicate a hack. iPhone and Android devices can check their battery use in their setting to check consuming power of apps and services. This can reveal whether any unidentified programmes are operating in the background. When you aren't actively using your phone, spyware and malware programmes run in the background, which might shorten the battery life. Hackers may use your social media accounts to send bizarre messages or publish information on your profile with malicious links. Getting notifications regarding unusual activity on your account may indicate that your device or account is in danger. Lowered screenshot quality, extremely high data usage can be other indicators of a hacked phone. If you see any of these signs, download a security programme that can check your device for dangers and eliminate threats. In the following paragraphs, we listed below some common mobile device threats and vulnerabilities (Weichbroth & Łysik, 2020).

- Theft of device
- Virus infection
- Data leakage
- Phishing and social engineering
- Phone hijacking
- Impersonation
- Message contamination
- Jail unlocking

4.1 Theft of device

Users save a wide variety of data, both personal and professional, on their mobile phones. We are more likely to lose our devices or have them taken by malicious people on Streets, Public Places, Office or Work, and Public Transport. The open medium, changing network topology, and lack of centralised administration make the environment for mobile devices susceptible to passive and active attacks. Owners of mobile devices pose the most risk to the security of sensitive data, but good behaviour on their part can mitigate this risk. The likelihood of losing sensitive data can be reduced by implementing 2FA (two-factor authentication), avoiding automatic logins, and employing password-lock programmes.

4.2 Virus infection

Malware authors focus has dramatically shifted from PCs to mobile devices as a result of the growing reliance on smartphone devices and the financial information they

store. Once a mobile is infected with virus (a type of malware), it can become a source for spreading viruses to other vulnerable devices by sending text messages and email. These text messages and emails can lead other users to open the malicious file which results in spreading virus to their phones. The more harmful malware has the ability to alter, copy, or erase important files as well as possibly infect business servers. Malicious software can spread to other devices and allow files to be stolen. Programmes like Cabir, Duts, Skulls, and DroidKungFu were created specifically to attack computers and mobile devices.

4.3 Data leakage

In general, a lot of malware samples gather the sensitive information kept on the mobile device and transport it to distant servers with ulterior motives. When financial credentials are targeted, this type of information leak assault may have a greater effect on the users. Some malware seeks to manipulate the mobile device for future exfiltration rather than causing an instant information breach on the stored data. The Trojan opens a back door for processing requests from a C&C (Command and Control) server once it has been installed on the infected device. Later, the Trojan places calls to premium numbers it has acquired via the C&C server. Making calls and sending SMS messages to premium lines may cause the user financial harm.

4.4 Phishing and social engineering

Mobile devices like tablets and smartphones have become a frequent target of traditional web-based attacks like phishing due to their increased popularity. In Phishing, hackers trick users to enter their credentials in fake websites or fake mobile applications. Spam emails, which are widely disseminated by cybercriminals, are the primary medium for phishing attempts. Hackers also take use of social media platforms to take advantage of mobile phone users. They execute phishing scams in order to get user's credentials and financial information to make money out of it.

4.5 Phone Hijacking

In Phone Hijacking or SIM hijacking, the cybercriminals hijack the phone number. These assaults give hackers access to all the accounts where the user's phone number is used in order to ensure authenticity. Attackers can get access to victim's calls, messages and other personal or Financial Information. It is advised to enable SIM lock, avoid clicking on suspicious links and sharing personal data via email. If you suspect phone hijacking, contact your service provider right away and ask them to lock your account.

4.6 Impersonation

An Impersonation attack is the one where the Cybercriminals pretend to be someone else in order to trick victims into disclosing personal information and target user to make a financial transfer. Cybercriminal use fake emails, apps to steal confidential information which can cost people and businesses a lot of money and steal sensitive data. These attacks are harder to identify and stop because, unlike typical cyberattacks, which frequently focus on taking advantage of technical flaws, they target the human factor. Before downloading any app, users should confirm its legitimacy, this will assist prevent mobile app impersonation.

4.7 Message Contamination

Message Contamination can happen in two ways-intentionally, when hackers try to get access to user's information, or unintentionally, which can occur as a result of technical error.

If the Message Contamination is Intentionally done then message can contain hidden codes in it which can lead to malware attacks resulting in compromising user's personal data. Just opening the message can activate these malicious codes which poses threat to the device security and user privacy, where sensitive information or data is revealed to the unauthorized third parties. Avoid opening messages from suspicious or unfamiliar sources and routinely update the security software.

4.8 Jail Unlocking

When users want to get more control over their devices in order to install unauthorize apps or improve functionality that are restricted by default, they remove restrictions imposed by their Operating Systems, can be referred to as Jail Unlocking. Jailbreaking make their devices more vulnerable to security risks and comprising user's data as security constraints are removed from the operating system. When downloading apps, stick to authorized sources and use legitimate app stores. Using biometric identification techniques, creating strong passwords, and encrypting the device can all be preventive measures.

By utilising anti-malware software, avoiding dubious links and downloads, and keeping devices updated with the most recent security patches and updates, using strong passwords and Secure Wi-Fi Networks, mobile users can take precautions to safeguard their devices from these attacks.

5. Conclusion

Phone hacking is a significant concern in today's world, where we rely heavily on phones for nearly every task, along with numerous services and applications. They may offer their own advantages, but they also have considerable drawbacks that accompany them. While technological developments have made it simpler to access and share information, they have also made it simpler for hackers to take advantage of flaws in mobile devices and networks. We reviewed common mobile hacking threats, such as Bluetooth, malware, keylogger, camera-based, as this literature analysis has demonstrated.

Organisations are depending more and more on mobile devices to improve productivity at work. Data breaches that are costly to the organisation, interrupt operations, and damage reputations can be caused by theft, infection, and careless usage of mobile devices. Hence, it is in the organisations' best interests to create and abide by safe mobile device practises. It is crucial to take a proactive approach to addressing these risks, which include having security measures in place like two-factor authentication, routinely updating software, and instructing people on safe practises. Also, it is important for companies creating mobile devices to give security as top priority so that created systems resist being hacked. In order to protect the privacy and security of sensitive information, it is crucial to be cautious and take precautions against phone hacking. Hence It is Advisable to use Security Software, Two factor Authentication technique, refrain from clicking on dubious links and messages, updating Software on regular basis, avoid using public Wi-Fi Networks or even if are using one try to refrain from accessing bank accounts or accessing sensitive information.

6. References

1. Ahmadi, S. (2023). Security And Privacy Challenges in Cloud-Based Data Warehousing: A Comprehensive Review. *International Journal of Computer Science Trends and Technology (IJCST)–Volume*, *11*.
2. Browning, D., & Kessler, G. C. (2009). Bluetooth hacking: A case study. *Journal of Digital Forensics, Security and Law*, *4*(2), 57. doi:10.15394/jdfsl.2009.1058
3. Dahiya, R., Kashyap, A., Sharma, B., Sharma, R. K., & Agarwal, N. (2024). Security in Mobile Network: Issues, Challenges and Solutions. *EAI Endorsed Transactions on Internet of Things*, *10*.
4. Halpert, B. (2004, October 8). Mobile device security. In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development (pp.99-101)*. doi:10.1145/1059524.1059545
5. He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications, 22(1),* 138–144. doi:10.1109/mwc.2015.7054729
6. Kar, A., Stakhanova, N., & Branca, E. (2024). Detecting Overlay Attacks in Android. *Procedia Computer Science, 231*, 137-144.
7. Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, *8*(1), 36-48.
8. Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*, *56*, 376-383.
9. Kim, Y., Oh, T., & Kim, J. (2015). Analyzing user awareness of privacy data leak in mobile applications. *Mobile Information Systems*, *2015*(1), 369489.
10. Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, *2*(3), 31-42.
11. Kuncoro, A. P., & Kusuma, B. A. (2018, November). Keylogger is a hacking technique that allows threatening information on mobile banking user. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)* (pp. 141-145). IEEE. doi:10.1109/icitisee.2018.8721028
12. Moses, A., & Morris, S. (2021). Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies. JISCR, 4(2), 103–131.
13. Muraleedhara, P., Christo, M. S., Jaya, J., & Yuvasini, D. (2024). Any Bluetooth device can be hacked. Know how?. *Cyber Security and Applications*, *2*, 100041.
14. Nagarjun, P. M. D., & Ahamad, S. S. (2018). Review of mobile security problems and defensive methods. *International Journal of Applied Engineering Research, 13(12),* 10256-10259.
15. Ruhani, A. B. B., & Zolkipli, M. F. (2023). Keylogger: The unsung hacking weapon. *Borneo International Journal eISSN 2636-9826*, *6*(1), 33-43.
16. Shahad, A. T., & Al-Haija, Q. A. (2024). Secure Mobile Payment (SMP): Challenges and Potential Solutions. *International Journal of Intelligent Systems and Applications in Engineering, 12(11s),* 103-120.
17. Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews, 21(2),* 1720-1736.
18. Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. *Mobile Information Systems*, *2020*(1), 8828078.
19. Wu, L., Du, X., & Fu, X. (2014). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications Magazine*, *52*(3), 80-87.

❖ ❖ ❖