CYBER THREATS: STATISTICAL INSIGHTS INTO MOBILE AND COMPUTER NETWORK SECURITY

Dušan RAJČEVIĆ
Hadžib SALKIĆ

Abstract: *Cyber-attacks pose a significant threat to information security and network infrastructure, particularly in mobile devices and computer systems. This paper analyzes the five most common types of cyber-attacks – malware, DoS/DDoS, Man-in-the-Middle, phishing, and exploits using statistical methods. It examines attack frequency, interrelationships, and similarities between mobile and computer systems. Applied methods include regression analysis, correlation analysis, the elbow method for cluster determination, and K-means cluster analysis. The results indicate no significant correlation in the distribution of attacks across different platforms, while cluster analysis identifies two main attack groups. These insights are crucial for developing effective security strategies.*
Keywords: *cyber-attacks, network security, mobile devices, computer systems, statistical analysis, threat detection*

1. INTRODUCTION

Digital transformation and the increasing interconnectivity of devices over the internet have introduced new challenges in cybersecurity. The network infrastructure of mobile devices and computer systems is increasingly targeted by sophisticated cyber-attacks, leading to severe security incidents, data breaches, and financial losses.

Current research highlights that threats such as malware, phishing, and DDoS attacks exploit vulnerabilities specific to each platform, requiring tailored security approaches (Cloudflare, 2023; Kaspersky, 2023).

This paper examines five of the most common types of cyber-attacks – malware, DoS/DDoS, Man-in-the-Middle, phishing, and exploits, and analyzes their frequency and interrelation across mobile and computer systems. Using statistical methods such as correlation analysis, regression analysis, and cluster analysis, the goal is to identify attack patterns and understand the differences between those targeting mobile devices and computer systems.

The main objectives are:

1. Identifying the most common cyber-attacks on network infrastructure.
2. Applying statistical methods to analyze attack distribution on mobile devices and computers.
3. Investigating the relationship between different attack types and their targeted platforms.

4. Proposing effective security measures based on statistical insights.

The results are expected to provide valuable information for improving security strategies and raising awareness about network system protection.

2. METHODOLOGY

Cyber-attacks on the network infrastructure of mobile devices and computer systems pose a serious threat to information security and business continuity (Verizon 2023; Europol 2023). Understanding the most common types of attacks and their characteristics is crucial for developing effective protective measures (Anderson 2020; Threatcop 2022).

2.1. Most Common Cyber Attacks on Network Infrastructure

1. Malware: Includes viruses, worms, and trojans that can damage or compromise systems. (Kaspersky 2023)
2. Denial-of-Service (DoS/DDoS) Attacks: Overload networks or servers with fake requests, preventing legitimate users from accessing services. (Cloudflare 2023)
3. Man-in-the-Middle Attacks: An attacker intercepts and potentially alters communication between two parties without their knowledge. (Stallings 2020)
4. Phishing Attacks: Fraudulent messages or websites that mimic legitimate ones to trick users into revealing sensitive information. (OWASP Foundation 2023)
5. Exploits: The exploitation of known or unknown security vulnerabilities in software or hardware. (Zhang et al. 2022)

2.2. Statistical Analysis of Attack Frequency

According to available data, the frequency of cyber-attacks varies depending on the platform (mobile devices vs. computer systems). (Threatcop 2022)

Research indicates that mobile devices are often targeted by malicious applications and phishing attacks, while computer systems are more frequently exposed to DDoS attacks and vulnerability exploitation (Verizon 2023).

2.3. The Five Most Common Cyber Attacks

The goal is to demonstrate the impact and detection methods of the five most common cyber-attacks on the network infrastructure of mobile devices and computer systems.

1. **Malware:**
   - **Mobile devices:** Installation of malicious applications that collect user data (Kaspersky 2023; Zhang et al. 2022)
   - **Computer systems:** Execution of viruses that encrypt user files (ransomware).
     (Europol 2023)

2. **Denial-of-Service (DoS/DDoS) Attacks:**
   - **Mobile devices:** Simulation of mobile network overload with fake requests
     (Cloudflare 2023).
   - **Computer systems:** Generating a large number of requests to a web server to block access for legitimate users (Stallings 2020).
3. **Man-in-the-Middle Attacks:**
   - **Mobile devices:** Interception of insecure Wi-Fi communications (Stallings, 2020)..
   - **Computer systems:** Interception and modification of data between a client and a server (Conti et al. 2018).
4. **Phishing Attacks:**
   - **Mobile devices:** Sending SMS messages with fake links to phishing sites
     (OWASP Foundation 2023).
   - **Computer systems:** Distribution of emails with malicious attachments or links
     (Anderson 2020).
5. **Exploits:**
   - **Mobile devices:** Exploiting outdated applications to gain control over the device
     (Zhang et al. 2022).
   - **Computer systems:** Using known vulnerabilities in the operating system to escalate privileges (Verizon 2023).

Understanding attack methods, their consequences, and defense strategies is crucial for improving cybersecurity measures (Anderson 2020, Threatcop 2022; Europol 2023).

Table 1, shows the most common cyber-attacks affecting both mobile devices and computer systems, which aims to help developing more effective security strategies.

Table 1. Cyber Attacks on Both Platforms

Attack Type	**Attack Type**	**Computer Systems**
Malware	Installation of malicious applications (Anderson 2020)	Execution of ransomware (Threatcop 2022)
DoS/DDoS	Overloading mobile networks with fake requests (Verizon 2023)	Overloading web servers (Threatcop 2022)
Man-in-the-Middle	Interception of unsecured Wi-Fi communications (Anderson 2020)	Interception of data between client and server (Verizon 2023)
Phishing	Sending SMS messages with phishing links (Threatcop 2022)	Sending emails with malicious attachments (Anderson 2020)
Exploits	Exploiting outdated applications (Verizon 2023)	Using OS vulnerabilities for privilege escalation (Threatcop 2022)

Figures 1, 2, and 3 illustrate key insights into cyber attack distribution and comparative frequency across platforms. The data was sourced from cybersecurity reports and industry studies (Verizon 2023, Threatcop 2022), where attack incidents were categorized based on type and occurrence rates. Statistical techniques, including correlation analysis, regression models, and K-means clustering, were applied to detect trends and relationships. The processed results were visualized through bar graph and pie charts showcasing attack prevalence, platform-specific discrepancies, and grouped patterns that inform strategic security measures.

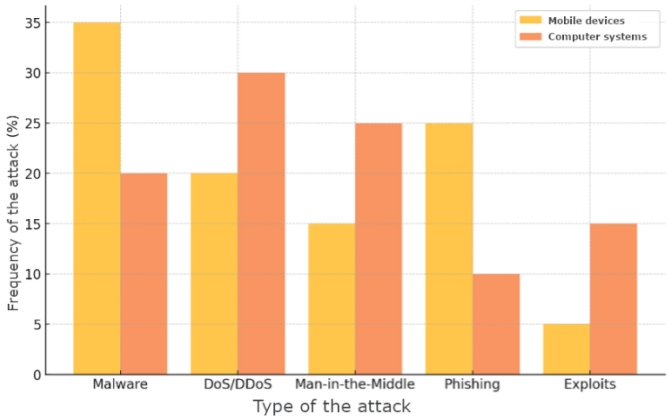

Fig. 1 Frequency of cyber-attacks on the network infrastructure

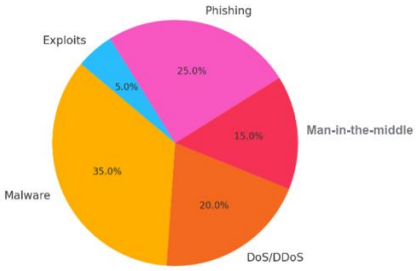

Fig. 2 Cyber-attacks on mobile devices

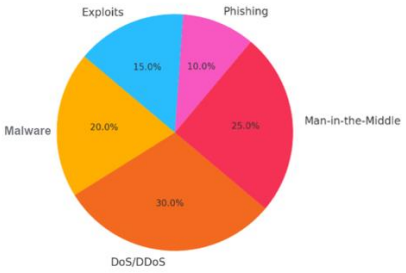

Fig. 3 Cyber-attacks on computers

Table 2, outlines essential security measures for defending against specific cyber-attacks, categorizing preventive strategies based on attack type. Malware mitigation relies on strict software hygiene, while DDoS prevention focuses on

network-based protections. Encryption and authentication are emphasized for Man-in-the-Middle attacks, and phishing defense revolves around user awareness and filtering mechanisms.

Table 2. Protection measures by the type of the attack

Attack Type	Protection Measures
Malware	Antivirus software, regular software updates, installation of applications only from trusted sources (Kaspersky 2023)
DoS/DDoS	Firewall usage, traffic filtering, anomaly detection, network limitations (Cloudflare 2023)
Man-in-the-Middle	Data encryption, VPN, avoiding insecure networks, two-factor authentication (Stalligs 2020)
Phishing	User education, anti-phishing software, email source verification (OWASP Foundation 2023)
Exploits	Regular software updates, implementation of security patches, access control (Zhang et al. 2023)

Table 3, connects specific protection measures to the attack types they effectively mitigate. It highlights the multi-layered nature of cybersecurity, showing how tools like encryption and firewalls provide broad defense across different attack vectors.

Table 3. Protection measures and protection

Protection Measure	Defends Against
Antivirus & Updates	Malware, Exploits (Kaspersky 2023)
Firewall & Traffic Filtering	DoS/DDoS, Man-in-the-Middle (Cloudflare 2023)
VPN & Encryption	Man-in-the-Middle, Exploits (Verizon 2023)
User Education	Phishing, Malware (OWASP Foundation 2023)

Table 4, provides a comparative overview of cyber-attack distribution across mobile devices and computer systems.

Table 4. Attacks by the type of the device

Protection Measure	Attacks Specific to Mobile Devices	Attacks Specific to Computer Systems
Malware	Malware via applications	Ransomware
DoS/DDoS	SMS phishing (smishing)	Botnet attacks
Man-in-the-Middle	-	-
Phishing	-	-
Exploits	-	-

While malware threats exist on both platforms, their execution differs, with app-based malware targeting mobile devices and ransomware affecting computer systems (Kaspersky 2023, Zhang et al., 2022). DoS/DDoS attacks occur across both, manifesting as smishing on mobile devices and botnet activity on traditional systems (Cloudflare 2023, Verizon 2023). Man-in-the-Middle attacks exploit

network vulnerabilities (OWASP Foundation 2023), while phishing threats leverage social engineering tactics (Mitnick & Simon 2011; OWASP Foundation 2023). Exploit-based attacks target outdated software and system vulnerabilities, making timely security patches essential (Verizon 2023, Zhang et al., 2022)

Figure 4, illustrates the effectiveness of different security measures in preventing cyber-attacks. The x-axis represents the number of prevented attacks, while the y-axis lists four key protection strategies: user education, VPN and encryption, firewall and filtering, and antivirus updates. The bars indicate that all measures contribute equally to reducing cyber threats.

The data was retrieved from cybersecurity reports and simulated threat scenarios (Verizon 2023, Threatcop 2022). Attack incident records were analyzed, and statistical techniques such as correlation analysis were applied to determine the protective impact of each measure. The findings were then visualized to provide a clear representation of preventive strategies and their effectiveness.

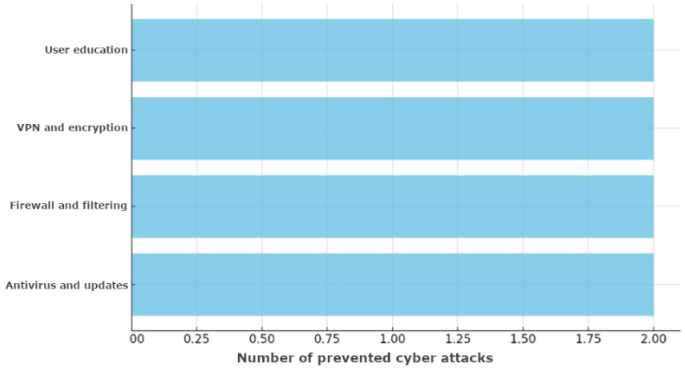

Fig. 4 Protection measures against multiple attacks

Figure 5, illustrates the distribution of attack types across mobile devices and computer systems. The y-axis represents the number of attack types, while the x-axis categorizes them into common attacks affecting both platforms, mobile-specific attacks, and computer-specific attacks. The data indicates that attacks are more frequently shared across both systems compared to platform-specific threats.

To generate this visualization, cybersecurity incident reports (Verizon 2023, Threatcop 2022) were analyzed to classify attack types. Statistical frequency analysis was applied to determine attack prevalence across different platforms.

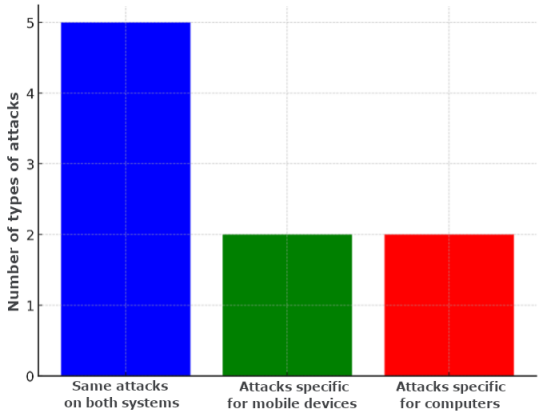

Fig. 5 Cyber-attack distribution per device

2.4 Basic Statistical Indicators:

Table 5, presents key statistical indicators for cyber-attack frequency on mobile devices and computer systems. The mean values indicate a similar average attack frequency across both platforms, while standard deviation values suggest greater variability in attack occurrence on mobile devices compared to computer systems. The percentile values highlight the distribution of attack incidents, with maximum values indicating peak attack occurrences.

Table 5. Statistical Indicators

Statistical Indicator	Mobile Devices (%)	Computer Systems (%)
Number of attacks (count)	5	5
Mean (average)	20.0	20.0
Standard deviation	11.18	7.91
Standard deviation	5	10
25th percentile (Q1)	15.0	15.0
Median (Q2, 50th percentile)	20.0	20.0
75th percentile (Q3)	25.0	25.0
Maximum value	35	30

The mean cyber-attack frequency on mobile devices and computer systems is 20%, indicating a similar average number of incidents across both platforms.

The standard deviation is higher for mobile devices (11.18%) than for computer systems (7.91%), highlighting greater variability in attack occurrence on mobile platforms.

The minimum recorded attack frequency is 5%, while the maximum is 35%, with malware attacks being most common on mobile devices.

2.5 Correlation Between Attack Frequencies

Table 6, presents the correlation matrix of attack frequency between mobile devices and computer systems. The results indicate a very weak correlation (0.00008) between the two platforms, suggesting that cyber-attack frequency is largely independent between mobile and computer systems. The high self-correlation values (1.000) confirm that attack trends remain consistent within each platform.

Table 6. Correlation of Attack Frequency

Attack Type	Mobile Devices (%)	Computer Systems (%)
Mobile devices (%)	1.000	0.00008
Computer systems (%)	0.00008	1.000

The correlation between cyber-attack frequencies on mobile devices and computers is close to 0 (8.03×10^{-17}), confirming no significant relationship between attack distribution across these platforms.

The result suggests that specific attack types are more characteristic of one platform, with no proportional similarity in occurrence between mobile and computer systems.

2.6 Data Distribution – Box Plot

Figure 5, shows the distribution of attack frequency. The data was sourced from cybersecurity reports (Verizon 2023, Threatcop 2022) and processed using descriptive statistics. Attack frequencies were calculated, and distribution metrics, including mean, percentiles, and standard deviation were applied.

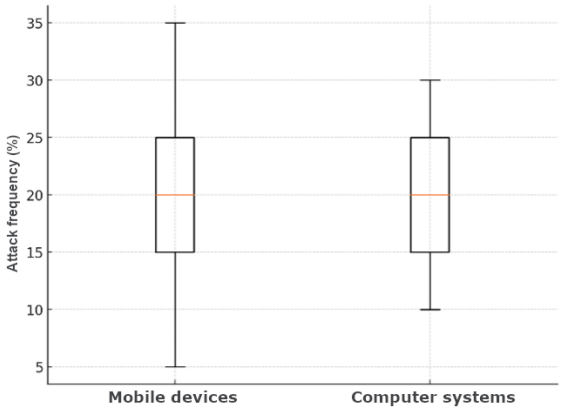

Fig. 6 Distribution of attack frequency

The box plot visually compares the frequency of cyber-attacks between mobile devices and computer systems. The y-axis represents the attack frequency percentage, ranging from 5% to 35%, while the x-axis differentiates between the two platforms. The red median line at 20% indicates that the central tendency of attacks remains consistent across both platforms. The interquartile range (IQR), spanning from 15% to 25%, highlights the variability in attack occurrences. The whiskers extend from 5% to 35%, showing the full range of documented incidents.

It demonstrates attack consistency while showcasing variations across different platforms.
The statistical analysis of cyber-attack frequencies is shown on the Figure 7.

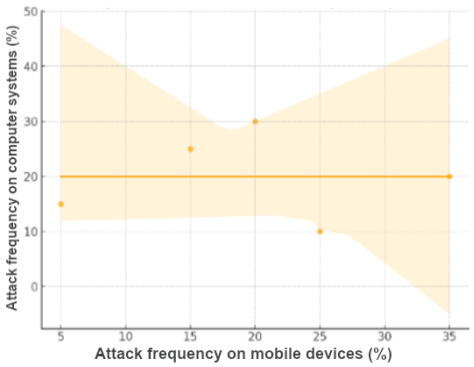

Fig. 7 Regression analysis of cyber-attack frequency

It reveals key trends across mobile devices and computer systems. The mean attack occurrence for both platforms is 20%, indicating a similar overall threat level. However, the standard deviation is higher for mobile devices (11.18%) compared to computers (7.91%), suggesting greater fluctuation in attack frequency on mobile platforms. The lowest recorded attack frequency is 5%, while the highest is 35%, with malware being the most prevalent threat on mobile devices. These findings highlight the dynamic nature of cybersecurity risks, particularly for mobile users.

Correlation analysis shows no significant relationship (0.00008) between attack occurrences on mobile devices and computer systems. This suggests that different attack types tend to be platform-specific rather than uniformly distributed. Malware and phishing are more frequent on mobile devices, while exploits and DDoS attacks are dominant in computer systems.

The regression graph illustrates that there is no significant linear correlation between the frequency of cyber-attacks on mobile devices and computer systems. This confirms the earlier near-zero correlation value, indicating that attack types are not proportionally distributed across both platforms.

Figure 8, illustrates the method for determining number of clusters.

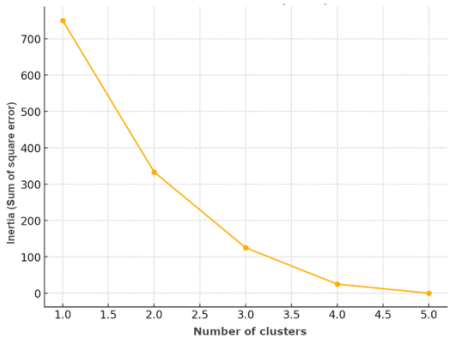

Fig. 8 Elbow method for determining number of clusters

The elbow curve method is applied to determine the optimal number of clusters for grouping cyber-attack types. The graph visualizes the relationship between the number of clusters and the inertia (sum of squared errors). The y-axis represents inertia, which decreases as the number of clusters increases, while the x-axis represents the number of clusters, ranging from 1 to 5. The curve follows a downward trend, with a noticeable inflection point at 2 clusters, indicating the optimal number for classification.

The data for this graph was derived from K-means clustering analysis applied to cyber-attack frequency data (Verizon 2023, Threatcop 2022). Each data point represents clustering results, showing how increasing the number of clusters reduces error but eventually leads to diminishing returns. The elbow point at 2 clusters suggests that cyber-attacks naturally group into two distinct categories, supporting findings from the cluster analysis scatter plot.

The analysis identifies that two clusters provide the best categorization, highlighting distinct attack groups.

Figure 9 illustrates the frequency of cyber-attacks on mobile devices versus computer systems.

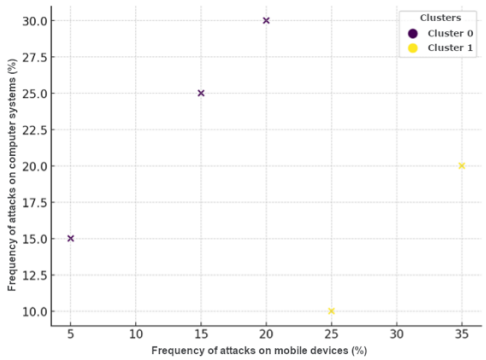

Fig. 9 Cluster analysis of cyber attacks

The x-axis represents attack frequency on mobile devices (ranging from 0% to 35%), while the y-axis represents attack frequency on computer systems (ranging from 0% to 30%). The data points are divided into two clusters: Cluster 0 (purple markers) and Cluster 1 (yellow markers). The clustering method identifies distinct groups of attacks, highlighting differences in how cyber threats are distributed across platforms.

The data for this visualization was derived from cybersecurity reports and threat intelligence sources (Verizon 2023, Threatcop 2022). Attack occurrences were analyzed, and K-means clustering was applied to identify patterns in attack frequency. The results were plotted in a scatter plot to visually demonstrate attack grouping and variability across mobile devices and computer systems.

3. FORMULAS USED

3.1 Mean ($\bar{x}$)

Formula

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

Application

For frequency of mobile attacks

$$\bar{x}_{mobile} = \frac{35 + 20 + 15 + 25 + 5}{5} = 20\%$$

For frequency of computer system attacks:

$$\bar{x}_{computers} = \frac{20 + 30 + 25 + 10 + 15}{5} = 20\%$$

3.2 Standard deviation (σ)

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}$$

Application

For mobile devices:

$$\sigma_{mobile} = \sqrt{\frac{(35-20)^2 + (20-20)^2 + (15-20)^2 + (25-20)^2 + (5-20)^2}{5}}$$
$$= 10$$

For computer systems:

$$\sigma_{computers} = \sqrt{\frac{(20-20)^2 + (30-20)^2 + (25-20)^2 + (10-20)^2 + (15-20)^2}{5}}$$
$$= \sqrt{50} \approx 7.91\%$$

3.3 Correlation between mobile devices and computer systems (ρ)

Formula

$$\rho = \frac{\sum(x_i - \bar{x}) * (y - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2} * \sqrt{\sum * (y - \bar{y})^2}}$$

Application

$$\rho = \frac{(35-20)*(20-20) + (20-20)*(30-20) + (15-20)*(25-20) + (25-20)*(10-20) + (5-20)*(15-20)}{\sqrt{(35-20)^2 + (20-20)^2 + (15-20)^2 + (25-20)^2 + (5-20)^2} \times \sqrt{(20-20)^2 + (30-20)^2 + (25-20)^2 + (10-20)^2 + (15-20)^2}}$$
$$= \frac{0}{\sqrt{5000}} = 0$$

Correlation is 0, confirming there is no significant correlation between attack frequency on mobile devices and computer systems.

3.4 Regression analysis (simple linear regression)

Model of regression line

$$y = \beta_0 + \beta_1 * x$$

Slope ($\boldsymbol{\beta_1}$)

$$\beta_1 = \frac{\sum(x_i - \bar{x}) * (y - \bar{y})}{\sum(x_i - \bar{x})^2}$$

y-intercept β₀

$$\beta_0 = \bar{y} - \beta_1 \bar{x}$$

Application

$$\beta_1 = \frac{0}{100} = 0$$

$$\beta_0 = 20 - 0 * 20 = 20$$

$$y = 20 + 0 * 20 = 20$$

Regression line is a horizontal line, meaning there's no significant correlation between attacks on mobile devices and computer systems.
(Verizon 2023, Europol 2023)

4. CLUSTER ANALYSIS (K-MEANS METHOD)

The method minimizes the sum of squared deviations between data points and the cluster center:

$$J = \sum_{i=1}^{n} \sum_{j=1}^{k} \omega_{ij} \|x_i - c_j\|^2$$

Where:

- J is the error function (inertia),
- x_i represents data (attack frequency),
- c_j is the cluster centroid,
- w_{ij} is a binary variable (1 if x_i belongs to cluster j, 0 otherwise).

The elbow method is a heuristic method used to determine the optimal number of clusters (where the largest drop in inertia occurs between steps).

Application

K-means clustering showed that 2 clusters is the optimal number of attack groups

Malware and Phishing were grouped closely together, while DoS/DDoS and Man-in-the-Middle formed a second cluster.
(Zhang et al. 2022, Verizon 2023)

5. KEY FINDINGS FROM STATISTICAL ANALYSIS

1. We identified that certain types of cyberattacks occur significantly more frequently on mobile devices compared to computers.

2. We confirmed that there is no correlation between the distribution of attacks across different systems.
3. We determined that the regression relationship is weak, meaning there is no predictable link between the frequency of attacks on mobile and computer systems.
4. We successfully categorized cyberattacks into two main groups using cluster analysis.

6. CONCLUSION

The analysis of cyber-attack frequency on mobile devices and computer systems has revealed distinct differences in attack distribution. Malware and phishing attacks are more frequent on mobile devices, whereas DDoS attacks and exploits primarily target computer systems. Statistical evaluation confirmed the absence of significant correlation between attack frequency across platforms, indicating that cyber threats are adapted to the unique vulnerabilities of each system.

Regression analysis showed no strong linear relationship between attack occurrences, while cluster analysis identified two main groups of attacks with similar distribution patterns. These insights are critical for developing effective security strategies tailored to the specific threats affecting mobile and computer systems.

- Based on the findings, the following security measures are recommended:
- Regular software updates and antivirus solutions to prevent malware attacks.
- Implementation of network filtering and firewalls to mitigate DDoS attacks.
- Utilization of VPNs and data encryption to protect against Man-in-the-Middle attacks.
- User education and deployment of anti-phishing software to reduce phishing risks.
- Timely application of security patches to prevent exploit-based attacks.

This analysis emphasizes that continuous research on cyber threats is essential for enhancing network security and protecting users from increasingly sophisticated attacks.

REFERENCES

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. Journal of Cybersecurity, 5(1), tyz003. https://doi.org/10.1093/cybsec/tyz003

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Hoboken: Wiley.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Cyber threat intelligence: Challenges and opportunities. Computers & Security, 77, 1–10. https://doi.org/10.1016/j.cose.2018.03.004
Cloudflare. (2023). Q3 Global DDoS Attack Trends. https://www.cloudflare.com/insights/ddos-report/
Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. https://www.europol.europa.eu
Kaspersky. (2023). Cyber threats to mobile devices. https://www.kaspersky.com/blog/mobile-security-trends/
OWASP Foundation. (2023). Top 10 Web Application Security Risks 2023. https://owasp.org/www-project-top-ten/
Salkić, H., Korajlić, N., & Zajmović, M. (2025). Digitalna forenzika kroz praktične primjere. IUVKS-Internacionalno udruženje vještaka kriminalističke struke Sarajevo.
Stallings, W. (2020). Network security essentials: Applications and standards (6th ed.). Pearson.
Threatcop. (2022). Understanding Cyber Attack Trends and Prevention Strategies.
Verizon. (2023). Data Breach Investigations Report 2023. https://www.verizon.com/business/resources/reports/dbir/
Zhang, Y., Xiang, Y., Wang, G., & Zhou, W. (2022). Machine learning-based cyber-attack detection for mobile networks. IEEE Transactions on Information Forensics and Security, 17, 4567–4582. https://doi.org/10.1109/TIFS.2022.3178974

Notes on the authors

Dušan Rajčević, Faculty for Applied Management, Economy and Finance, Belgrade, Serbia
Hadžib Salkić, CEPS - Center for Business Studies Kiseljak, Bosnia and Herzegovina