Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

Evaluation of Data Exposure Risks on Unencrypted Application Layer Protocols in RT/RW Net "X" Community Network Using NIST SP 800-86 Framework

Reza Febriana[1)], Muhammad Sidik Asyaky[2)]

[1)2)]Informatics, Siliwangi University, Indonesia
[1)]rezafebriana@unsil.ac.id, [2)] asyaky@unsil.ac.id

ABSTRACT

Security vulnerabilities in community-based networks, such as RT/RW Net, remain a critical concern due to the widespread use of unencrypted protocols. This study presents a quantitative evaluation of data exposure risks in application-layer protocols, focusing on HTTP traffic in local community networks. Using a network forensics approach based on the NIST SP 800-86 framework, traffic was captured and analyzed to measure the frequency and magnitude of sensitive data leaks using automated tools for network traffic analysis. The study quantified exposure across four key indicators: user credentials, session tokens, cookies, and personal information. The results indicated a high level of exposure, with analyzed HTTP packets successfully revealing sensitive data in plaintext, including usernames and passwords. Furthermore, statistical analysis of communication patterns identified significant opportunities for eavesdropping and session hijacking due to the lack of encryption standards. This evaluation provides empirical evidence of critical security gaps in RT/RW Net infrastructure and emphasizes the urgent need to transition to encrypted protocols (HTTPS). The findings provide a quantifiable risk assessment that can serve as a basis for implementing mitigation strategies in community-scale network management.

Keywords: Network; http; NIST; protocol; traffic

INTRODUCTION

The rapid development of computer network technology has shifted digital communication into a primary necessity in modern society. In network architecture, the Application Layer of the OSI and TCP/IP models plays a crucial role as the direct interface between users and network infrastructure. The Hypertext Transfer Protocol (HTTP) remains the fundamental protocol for client-server communication on the web. However, the persistent use of unencrypted HTTP in community-based networks, such as RT/RW Net "X," presents significant security risks, as sensitive data is transmitted in plaintext format (Basile & Lioy, 2015).

While threats to the HTTP protocol are well-documented, previous studies have largely focused on technical reports that are descriptive and demonstrative in nature, lacking measurable quantitative risk assessments. Consequently, a significant limitation exists in prior research regarding the absence of evaluations conducted through standardized frameworks and evaluation metrics (Wicaksana et al., 2025).

This research aims to address these limitations by performing a quantitative evaluation of data exposure risks using the NIST SP 800-86 framework. Distinct from conventional network forensic analysis, this study integrates a systematic investigation methodology stages to generate numerical data regarding the frequency and probability of sensitive data leakage, such as user credentials and session tokens (Kent et al., 2006).

RT/RW Net operates as a community-based local infrastructure designed to facilitate shared internet access for diverse activities, including web browsing, streaming, and online financial transactions. However, the organic growth of user density within these networks introduces critical challenges regarding performance stability and more pivotally information security (Mukhti et al., 2025).

The complexity of the problem is exacerbated by the fact that many RT/RW Net deployments, such as the one observed in “X” Community Network, lack centralized supervision and standardized security protocols. This regulatory and technical void leads to a systematic neglect of data privacy, transforming these community hubs into high-risk environments for cyber-attacks (Kusuma & Hasan, 2025).

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

In the absence of encryption at the application layer, the network's architectural vulnerabilities provide a broad attack surface for data exfiltration. Consequently, there is an urgent need for a quantitative evaluation to measure the actual magnitude of these risks (Rawat et al., 2023). By employing the NIST SP 800-86 framework, this study moves beyond qualitative assumptions to provide an empirical, forensic-based assessment of data exposure, specifically focusing on how unencrypted protocols fail to protect sensitive user information in unmanaged community infrastructures. This study also introduces the proposed Quantitative Risk Model for Community Networks, an evaluation model that goes beyond conventional descriptive analysis. The novelty of this study lies in the transformation of raw forensic data into measurable security metrics through the integration of the NIST SP 800-86 framework with the Weighted Risk Scoring system. This approach enables objective risk classification, providing an empirical basis for community network managers to prioritize mitigation on the most critical data assets.

LITERATURE REVIEW

RT-RW Net (*Rukun Tetangga-Rukun Warga Network*) is an information technology trend that provides internet services with a broader reach than internet cafes (Danang & Setiawan, 2022). This concept focuses on building internet network infrastructure at the local community level, such as in residential areas or villages/sub-districts (Februariyanti, 2008).

This research specifically focuses on the domain of Network Forensics, a specialized subset of digital forensics dedicated to the systematic integration and analysis of network traffic. While conventional network forensics often focuses on gathering legally valid evidence for post-incident investigation (Patil & Devane, 2022).

The analytical framework of this study is grounded in the OSI (Open Systems Interconnection) reference model, specifically focusing on the Application Layer (Layer 7). While the OSI model serves as a universal standard for heterogenous network communication, in the context of network forensics, it provides a structured taxonomy for identifying where sensitive data interactions occur. Specifically, research on the OSI model has only been conducted at the Application layer. This layer is the topmost layer in the OSI model, directly interacting with user applications. This layer provides network services for everyday activities, such as browsing, email, file transfer, and remote communication (Sushmita Biya & Renuka Uday Kotwal, 2023).

The NIST SP 800-86 framework, titled "Guide to Integrating Forensic Techniques into Incident Response," provides a standardized and rigorous methodology for performing digital forensic investigations. Unlike ad-hoc technical observations, this framework ensures that the forensic process is repeatable, reliable, and scientifically sound In the context of evaluating data exposure risks, NIST SP 800-86 offers a structured four-phase workflow: Collection, Examination, Analysis, and Reporting (Kent et al., 2006).

Previous studies have mostly focused on qualitative vulnerabilities without standardized quantitative metrics, but rather are only descriptive and demonstrative without quantifiable probability metrics. So no one has implemented a structured forensic framework like NIST SP 800-86 to obtain a quantifiable level of exposure. Therefore, this study provides a quantitative estimate of the likelihood of a data breach in identifying threats in the community network ecosystem through the proposed Quantitative Risk Model for Community Networks.

METHOD

The methodology of this research follows the NIST SP 800-86 framework, utilizing network traffic packet analysis as the primary instrument for quantitative evaluation. This framework, published by the National Institute of Standards and Technology (NIST), is designed to provide guidance in the digital forensics process. (Kent et al., 2006). Unlike traditional sniffing techniques that focus merely on data observation, this study employs systematic packet capture to provide a baseline for traceback and risk measurement within the community network environment (Dodiya & Singh, 2022). Implementing the NIST SP 800-86 framework ensures that digital forensics processes are conducted with methodological consistency and scientific rigor. This framework establishes a verifiable chain of evidence and an empirical basis, transforming raw packet data into measurable security metrics, enabling the methodology to go beyond mere technical demonstrations. By following a standardized four-phase investigation (collection, examination, analysis, and reporting). Then the process flow based on the methodology in this study is as shown in Fig. 1

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

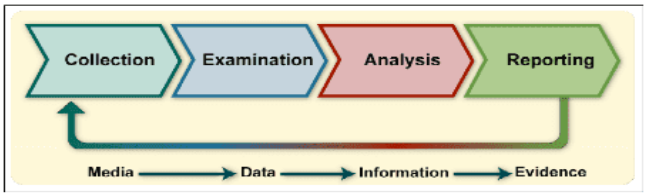

Fig. 1 Research methods based on NIST SP 800-86 framework

Collection

The data collection phase is carried out systematically using the Passive Sniffing technique via Port Mirroring on the core switch in the RT/RW Net "X" infrastructure, which is implemented on the Ethernet WAN/LAN interface (Eth02) on the router to ensure comprehensive packet visibility without sacrificing network performance (Al Manshury, 2023). This strategic sampling process was conducted over three time periods—morning, afternoon, and evening—with a capture duration of 10 minutes each (a total of 30 minutes), resulting in three representative Packet Capture (.pcap) files to capture traffic variations during peak hours. To ensure the accuracy of a rigorous quantitative risk evaluation, packet identification focused on unencrypted application layer protocols using Wireshark 4.0.x with a specific filter parameter of tcp.port == 80 (HTTP) to isolate sensitive data traffic transmitted in plaintext format.

Sampling was justified by setting three time window strategies to ensure an objective representation of traffic loads: a morning session (8:00–8:10 AM) to represent administrative activities and the beginning of daily usage, an afternoon session (1:00–1:10 PM) to monitor intermediate workloads, and an evening session (8:00–8:10 PM) to capture peak hour profiles where entertainment and personal transaction activity peak. As a form of bias control, data collection was limited to weekdays (working days) to avoid seasonal traffic anomalies that commonly occur on holidays. Furthermore, data integrity was maintained through the implementation of passive observation without intervention on normal user activity, so that the recorded network traffic behavior remains authentic and reflects the actual data exposure risk on the infrastructure.

Examination

The examination phase involves the systematic identification and extraction of relevant data from large-scale network traffic by isolating unencrypted application layer protocols, specifically HTTP on Port 80. This study employs automated scripts such as Python-Scapy to perform bulk extraction of specific forensic indicators. These indicators include HTTP Request Methods (POST/GET), User-Agent strings, session cookies, and sensitive payloads containing user credentials. This automated approach ensures high precision in identifying vulnerabilities and preparing the dataset for a comprehensive quantitative evaluation of data exposure risks.

Analysis

The data analysis phase of this study uses a formal statistical approach to achieve a quantifiable risk assessment of the RT/RW Net 'X' community network infrastructure. The process begins with an exposure rate calculation, where the percentage of sensitive packets exposed is explicitly compared to the total volume of captured HTTP traffic to generate an accurate interception probability matrix. Next, a frequency analysis is performed to map the density of data exposure into several key categories, including user credentials, session tokens, and other personally identifiable information (PII) transmitted in plaintext. The magnitude of the risk is then determined by integrating these probability calculations into a systematic risk assessment matrix, which evaluates severity based on the empirical impact of a potential data breach within the community.

Reporting

The final phase of this study follows the Reporting Phase of the NIST SP 800-86 framework, where forensic findings are synthesized into a formal scientific presentation. This phase prioritizes advanced data visualization of raw packet captures, using statistical tables to represent the identified risk landscape. These findings are processed using percentage formulas and translated into quantitative metrics, primarily the Data Exposure Rate, which serve as the empirical basis for the security recommendations provided in this study. This reporting provides empirical justification for necessary security interventions. These strategic recommendations are derived directly from the numerical evidence discovered during the analysis within the RT/RW Net 'X' community infrastructure. This evidence-based reporting ensures that the proposed mitigation strategies are technically validated and align with industry-standard cybersecurity practices.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

Research scenario in conceptual data collection

This scenario is used to capture network traffic using Passive Network Eavesdropping, a data collection technique in which researchers monitor and capture network traffic without modifying data packets or disrupting network operations. In the context of community infrastructure (RT/RW Net 'X'), This scenario is used to capture network traffic using Passive Network Eavesdropping, a data collection technique in which researchers monitor and capture network traffic without modifying data packets or disrupting network operations. In the context of a community infrastructure (RT/RW Net 'X'), this scenario simulates a threat where a malicious actor can reside on the same network and intercept sensitive citizen information transmitted over insecure protocols. This scenario is implemented to obtain a realistic picture of application layer vulnerabilities, as illustrated in Fig. 2.

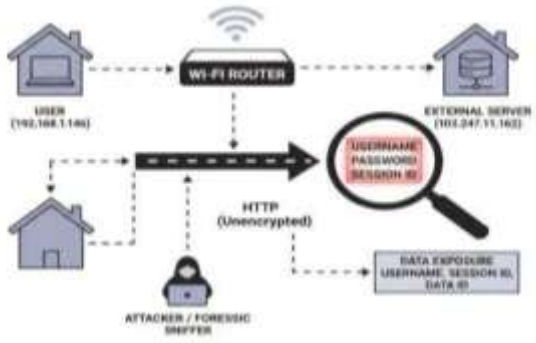

Fig. 2 Illustration of the research scenario in conceptual data collection

Detail Automated Forensic Script and Data Processing

To ensure reproducibility and minimize human error during data extraction, this study employed a Python-based script utilizing the Scapy library. The script was designed to perform batch processing on packet capture (.pcap) files with the following logical workflow:

Algorithmic Logic (Pseudo-code)

- Directory Iteration: Scanning the source folder to detect all captured .pcap files.
- Packet Processing: Reading packets sequentially and performing filtration based on the OSI layers:
  - Processing only packets that contain IP, TCP, and Raw Payload layers.
- Payload Inspection:
  - Decoding the raw data payload into string format (using error-ignore handling for non-standard characters).
  - Verifying the presence of the HTTP protocol within the payload.
- Extraction & Classification:
  - Identifying the request method (POST vs. GET).
- Performing pattern matching on strings to detect:
  - Credentials: Keywords such as user, pass, login, and pw.
  - Session Tokens: Keywords such as cookie and sessionid.
- Forensic Metadata Logging: Recording the Source IP, Destination IP, and exposure status for each packet meeting the specified criteria.
- Metric Calculation: Computing total traffic, the number of HTTP packets, and the Data Exposure Rate (DER) value.
- Data Export: Saving the final results into a structured format (CSV) for further statistical analysis.

Network Traffic Composition

The initial analysis focused on the network traffic composition the RT/RW Net “X” infrastructure. This inspection phase generated a substantial dataset for quantitative evaluation derived from three Packet Capture (.pcap) files totaling 16,816 captured network packets (Khaerullah & Mustofa, 2024).

The application of the network forensics script in this study resulted in a structured dataset that was extracted and

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

stored in the forensic_results.csv format. This file records important technical parameters of each analyzed packet, including the source and destination IP addresses, the HTTP method used, and the credentials exposure classification (credentials_exposed) from three Packet Capture (.pcap) files generated from the collection phase consisting of rtrw_morning.pcap, rtrw_afternoon.pcap, and rtrw_evening.pcap. The aggregate data in these files serves as the evidence base for validating the Data Exposure Level (DER).

Statistical Analysis Methods

To objectively measure the level of vulnerability at the application layer, this study used the Data Exposure Rate (DER) metric, formerly known as Sensitive Data Exposure. This metric is calculated by comparing the number of packets containing exposed sensitive information to the total number of unsecured protocol packets analyzed within a given period. The equation used to calculate the DER value refers to OWASP A02:2021 for measuring cryptographic failures on sensitive information, which is formulated as follows (OWASP Foundation, 2021):

$$DER = \frac{\sum_N Exposed}{\sum_N Total} 100\% \quad (1)$$

Information:

- $\sum_N Exposed$: Number of packets detected containing sensitive data / Credentials Exposed (171 packets)
- $\sum_N Total$: Total HTTP packets Analyzed (307 packets)

Weighted risk scoring

The classification of the level of danger in this infrastructure network is based on a threshold parameter that measures the correlation between the percentage of DER and the frequency of credential events, which is presented systematically in Table 1 (Rocco S. & Ramirez-Marquez, 2011).

Table 1
Risk Classification Thresholds

Risk Level	DER Threshold	Credential Exposure	Implication
Low	< 10%	< 10 instances	Minimal risk of data breach
Medium	10% - 30%	10 - 50 instances	Moderate risk; requires attention
High	> 30%	> 50 instances	Critical risk; immediate action required

Diagram Pipeline

The data transformation procedure from raw packets to quantitative risk metrics is carried out through a systematic pipeline designed to ensure the integrity and accuracy of the analysis, as illustrated in the following pipeline diagram.

Fig. 3 Pipeline Diagram

Pipeline Explanation

- Port Mirorring (PCAP): The starting point where all traffic captured through port mirroring is stored as raw digital assets for analysis.
- Filtering (Python-Scapy): A critical step to ensure reproducibility. The script cleans up corrupted or duplicated packets, allowing only valid data to be processed.
- Parsing: The process of unpacking packets to reveal the payload content. The primary focus is on POST methods (usually containing form/login submission data) and GET methods (containing URL parameters).
- Classification: Successfully extracted data is automatically separated into sensitivity categories:
  - Credentials: Username and password.
  - Session Token: Active access key.
  - PII: Personally identifiable information.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

- Metadata: Non-sensitive supporting information.

- Metric Calculation: The final stage of the quantitative evaluation where a DER score is calculated based on the percentage of exposure, and Weighted Risk Scoring assigns a weighting of the severity of each detected category.

RESULT

Based on the research, traffic data was captured when users accessed various websites through the RT/RW Net XYZ network. At this stage, all ongoing communications were recorded using a pre-designed scenario, with the following results (Arief et al., 2025):

Packet Capture Statistics

Network forensic Script results of data exposure a substantial dataset for quantitative evaluation. As shown in Fig. 3, the data consisted of a total of 16,816 captured network packets. Within this total traffic volume, 307 packets were identified as unencrypted HTTP packets, and most significantly, the forensic process successfully extracted 171 packets identified as containing sensitive data, including plaintext credentials.

Fig. 4 Network forensic Script results of data exposure

The overall results of the quantitative assessment are summarized in Table 1, which presents the key metrics used to evaluate the extent of data exposure within the monitored community network.

Table 2
Quantitative Metrics of Data Exposure Evaluation

Metric Category	Data Source (pcap)	Value	Total / Percentage
Total HTTP packets Analyzed	All Sessions	307	100%
Credentials Exposed	rtrw_morning.pcap	5	171
	rtrw_afternoon.pcap	68	
	rtrw_evening.pcap	98	
Not Credentials Exposed	rtrw_morning.pcap	1	136
	rtrw_afternoon.pcap	81	
	rtrw_evening.pcap	54	
Session Tokens Exposed	All Sessions	3	3

The results of a quantitative analysis of data traffic on the tested network showed a total of 307 HTTP packets analyzed across all sessions (All Sessions) spanning three different time periods (morning, afternoon, and evening). All these packets were evaluated to detect the presence of sensitive information transmitted without encryption.

A total of 171 credential packets were also found to be exposed in plaintext, with the highest distribution occurring in the daytime session (rtrw_evening.pcap) with 98 packets. This indicates that peak user activity at that time is linearly correlated with emerging security risks.

In addition to credentials, the identification of 3 Session Tokens Exposed confirmed a critical security flaw that could enable session hijacking attacks. Even from a network forensics perspective, the payload data section is often the richest source of evidence, as it can contain sensitive information such as user credentials, form submissions,

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

downloaded files, or specific web content, such as one of the session tokens exposed in this study, which revealed username and password credentials, as seen in Fig. 4.

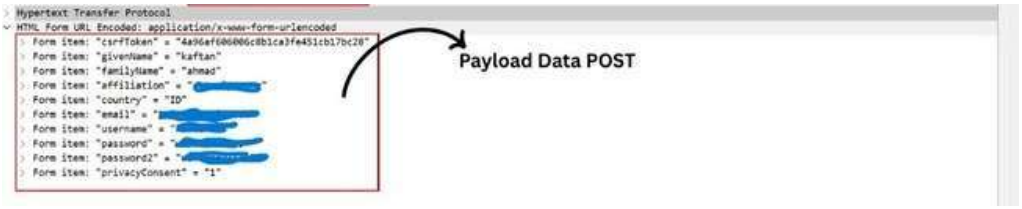

Fig. 5 Payload Data in Session Tokens Exposed

The main weakness identified was not only the lack of encryption, but also the failure of real-time incident detection. From a network forensics perspective, the exposure of session tokens seen in (Fig. 5) is the most concerning finding as it allows session hijacking without requiring further user interaction.

Quantitative Analysis of Network Vulnerability

Based on the results of quantitative metric calculations, this study recorded a Data Exposure Rate (DER) with a value of 55.70%, it can be concluded that the percentage of exposed credentials is 55.70% and the remaining unexposed credentials is 54.30% as shown in the graph in Figure 6. This figure is obtained from the accumulated ratio of 171 credential packets including 3 exposed session tokens compared to a total of 307 HTTP packets analyzed during the observation period. Statistically, a DER value exceeding the 50% threshold indicates that most sensitive data transmissions on the tested network are in an unencrypted state (plaintext), making them highly vulnerable to passive eavesdropping and man-in-the-middle (MitM) attack techniques. This finding confirms that without the implementation of additional security layers such as Transport Layer Security (TLS), the integrity and confidentiality of user data in the network infrastructure are at a critical risk level.

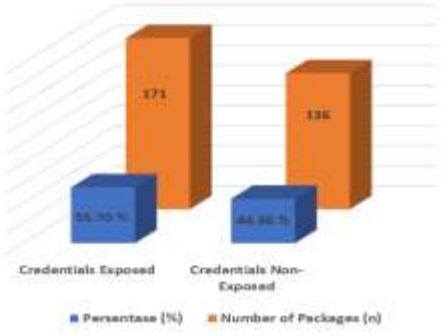

Fig. 6 Data Exposure Rate (DER) Graph

Weighted Risk Score Results

Based on the risk classification threshold reference in Table 1, the evaluation results indicate that the network vulnerability level is in the worrying category with a Data Exposure Rate (DER) value reaching 55.70%, which automatically places it in the HIGH risk classification (score 5). This critical condition is emphasized by the discovery of 171 incidents of user credentials being exposed in plain text format, which also occupies a HIGH risk level. Meanwhile, although the number of Session Tokens exposed is much smaller, namely 3 incidents, this category is still classified at a MEDIUM risk level (score 3) due to its potential impact on user session hijacking. Overall, the quantitative metrics from the 307 analyzed HTTP packets provide empirical evidence that the network infrastructure has significant security vulnerabilities and requires immediate mitigation action.

DISCUSSIONS

Analyzing the High Data Exposure Rate (DER): The Failure of Confidentiality

The results of this study reveal that the security risk in the RT/RW Net "X" infrastructure is at a critical level, as evidenced by the Data Exposure Rate (DER) of 55.70%. The calculated Data Exposure Rate (DER) of 55.70% (Table

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

1) provides empirical evidence of a widespread failure in achieving information security within this specific community network. When viewed through the lens of the fundamental CIA Triad (Confidentiality, Integrity, Availability) model, these results directly signify a profound breach of Confidentiality (Shoufan & Damiani, 2017).

This finding makes an important contribution to the network forensics literature by providing a quantitative measurement, going beyond the descriptive analysis that has dominated similar case studies. Specifically, the identification of 171 credential packets and 3 session tokens in plaintext indicates that the application-level protection mechanisms in the community network are very fragile.

Within this total traffic volume, 307 packets were identified as unencrypted HTTP application-layer traffic, which became the primary focus for in-depth packet inspection using a custom network forensic script. The automated analysis revealed a critical security landscape, specifically identifying five unencrypted POST requests and three exposed session tokens that could potentially facilitate session hijacking attacks (Krasser et al., 2005).

Compared to previous research by (Wicaksana et al., 2025) which also highlighted HTTP vulnerabilities on public networks, this study also highlights HTTP vulnerabilities on public networks but more specifically for RT/RW Net community networks. This study also provides added value through the application of the NIST SP 800-86 framework which allows for systematic extraction of forensic indicators and uses automated scripts (Scapy-Python) to perform network forensic processes. Data patterns show that nighttime sessions have the highest exposure rate (98 packets), which statistically proves a correlation between the amount of traffic and the chance of successful eavesdropping.

Insight: Driving Factors Behind the High DER

The high exposure rate can be attributed to two main intersecting factors: infrastructure-level decisions and user behavior.

Infrastructural Decisions: The root cause of the widespread exposure is the reliance on unencrypted HTTP (Port 80) across the core network infrastructure, particularly at the gateway where port mirroring was conducted. While major global platforms use HTTPS, many local/internal applications (e.g., local login pages, simple content servers) within these community networks do not. The lack of pervasive TLS/SSL encryption implies a lack of defensive measures at the application layer, allowing a passive sniffer to achieve comprehensive visibility without having to bypass any cryptographic protections.

User Behavior and Activity Patterns: Table 2 clearly illustrates that the highest volume of exposed indicators occurs during the Evening Session (20:00 - 20:30), coinciding with peak personal internet use. This trend strongly suggests that user behavior plays a significant role in increasing the net risk of exposure. Users are likely to perform logins, fill out personal information (PII) forms, or manage session-based accounts after standard working hours, creating a massive influx of sensitive data transmissions. The combination of unencrypted infrastructure and high-volume user activity creates the "perfect storm" that results in a high DER, maximizing the attack surface during peak hours.

Implications for RT/RW Net Governance (Policy and Practice)

These findings have severe implications for the current governance models often employed by community-based network providers like RT/RW Net.

Urgency for Application-Layer Encryption: The primary technical implication is the need for an enforced policy to migrate any local network applications (such as administrative login portals or local service platforms) from HTTP to HTTPS using widely available, free certificates (e.g., Let's Encrypt). Relying solely on perimeter security is insufficient when confidentiality is fundamentally broken within the local broadcast domain.

Formalizing Security Governance: Most RT/RW Net operators prioritize cost-efficiency and connectivity over security. The empirical data provided by this research justifies a shift toward formalizing security as a pillar of their operations. Governance structures must include minimum security standards that address the Confidentiality failure identified here, moving away from a purely reactive stance toward a proactive risk management approach. Failure to do so exposes the community network's user base to significant, verifiable risks of identity theft and credential compromise.

CONCLUSION

This study successfully conducted a comprehensive assessment of data exposure risks within community-based networks (RT/RW Net) using an automated forensic-based pipeline. Based on the findings, several key conclusions are drawn:

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

The primary contribution of this research is the establishment of the first quantitative forensic-based evaluation in community networks. While previous studies often relied on qualitative surveys or general descriptions, this research provides empirical, packet-level evidence of security vulnerabilities. The identification of a 55.70% Data Exposure Rate (DER) and the high frequency of credential leaks (171 instances) categorize the current state of RT/RW Net governance as High Risk, highlighting a critical failure in maintaining the Confidentiality of user data.

Policy recommendation

The practical implications of this research suggest an urgent need for a shift in network governance. From a policy perspective, community network providers must move beyond mere connectivity and adopt security-by-default policies. We recommend that local network operators implement mandatory TLS/SSL encryption for all local administrative portals and provide basic cybersecurity awareness for users. This study serves as a foundational benchmark for future research to develop more resilient and privacy-respecting community network architectures.

REFERENCES

Al Manshury, M. S. (2023). Penggunaan Software Wireshark untuk Monitoring dan Troubleshooting pada Komunikasi Client Server IEC 61850. *ELECTRON Jurnal Ilmiah Teknik Elektro*, *4*(2), 62–69.

Arief, A. R. W., Wisnu, M. W. H., Yanti, H. A., & Fauzi, A. F. Z. (2025). Analisis Vulnerabilitas HTTP pada Jaringan Publik Menggunakan Wireshark. *Journal of Informatics and Communication Technology (JICT)*, *7*(1), 198–209.

Basile, C., & Lioy, A. (2015). Analysis of Application-Layer Filtering Policies With Application to HTTP. *IEEE/ACM Transactions on Networking*, *23*(1), 28–41. https://doi.org/10.1109/TNET.2013.2293625

Danang, D., & Setiawan, K. (2022). Pengaturan Billing Hotspot Pada Sistem Jaringan Rt/Rw Net Dengan Mikrotik Router Os. *Januari*, *1*(1).

Dodiya, B., & Singh, U. K. (2022). Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise. *International Journal of Computer Applications*, *183*(53), 1–6. https://doi.org/10.5120/ijca2022921876

Februariyanti, H. (2008). Internert Murah dengan Membangun Jaringan RT-RW Net. *Jurnal Teknologi Informasi DINAMIK*, *xlll*(2), 98–114.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *The National Institute of Standards and Technology*.

Khaerullah, S. M., & Mustofa, D. (2024). Penggunaan Wireshark Dalam Penyadapan Lalu Lintas Data Berprotokol Http Pada Jaringan Wi-Fi. *Jurnal Ilmiah IT CIDA*, *10*(1), 19. https://doi.org/10.55635/jic.v10i1.203

Krasser, S., Conti, G., Grizzard, J., Gribschaw, J., & Owen, H. (2005). Real-time and forensic network data analysis using animated and coordinated visualization. *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 42–49. https://doi.org/10.1109/IAW.2005.1495932

Kusuma, M. R., & Hasan, M. Z. (2025). Strengthening Security in RT/RW Community Networks: A Case Study on Router Default Configuration Vulnerabilities in Indonesia. *JOISTECH: Journal of Information System and Technology*, *2*(2), 46–52.

Mukhti, D. A., Fitriana, Y. B., Yuwono, D. T., & W., Y. (2025). Analisis Kinerja Layanan RT/RW.NET Robby Media Berbasis Hotspot Menggunakan Metode Quality of Service. *Digital Transformation Technology*, *5*(1), 23–32. https://doi.org/10.47709/digitech.v5i1.5549

OWASP Foundation. (2021). *OWASP Top 10:2021 – A02:2021 – Cryptographic Failures*. https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Patil, R. Y., & Devane, S. R. (2022). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. *Journal of King Saud University - Computer and Information Sciences*, *34*(5), 2031–2044. https://doi.org/https://doi.org/10.1016/j.jksuci.2019.11.016

Rawat, R., Chakrawarti, R. K., Raj, A. S. A., Mani, G., Chidambarathanu, K., & Bhardwaj, R. (2023). Association rule learning for threat analysis using traffic analysis and packet filtering approach. *International Journal of Information Technology*, *15*(6), 3245–3255. https://doi.org/10.1007/s41870-023-01353-0

Rocco S., C. M., & Ramirez-Marquez, J. E. (2011). Vulnerability metrics and analysis for communities in complex networks. *Reliability Engineering and System Safety*, *96*(10), 1360–1366. https://doi.org/10.1016/j.ress.2011.03.001

Shoufan, A., & Damiani, E. (2017). On inter-Rater reliability of information security experts. *Journal of Information Security and Applications*, *37*, 101–111. https://doi.org/10.1016/j.jisa.2017.10.006

Sushmita Biya, & Renuka Uday Kotwal. (2023). The OSI Model: Overview of All Seven Layers of Computer

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/ 10.47709/cnahpc.v8i2.8014

Submitted : 2026-02-14
Accepted : 2026-04-07
Published : 2026-04-09

Networks. *International Journal of Advanced Research in Science, Communication and Technology*, *4*(3), 427–432. https://doi.org/10.48175/ijarsct-13064

Wicaksana, A. R., Haryanto, M. W., Yanti, H. A., & Zayandra, A. F. (2025). Analisis Vulnerabilitas HTTP pada Jaringan Publik Menggunakan Wireshark. *Journal of Informatics and Communications Technology (JICT)*, *7*(1), 198–209. https://ejournal.akademitelkom.ac.id/j_ict/index.php/j_ict/article/view/451

* Corresponding author