IJMRSETM

e-ISSN: 2395 - 7639

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

Comparative Study of NGFW and UTM Devices in SMB Security Infrastructures

Syed Zain R. Rizvi

University of Calgary, Calgary, AB, Canada

ABSTRACT: As small and medium-sized businesses (SMBs) increasingly adopt internet-facing applications and cloud-based services, securing their networks becomes both a necessity and a challenge. Limited budgets, constrained IT staffing, and growing attack surfaces demand cost-effective yet comprehensive security solutions. This paper presents a comparative evaluation of two widely adopted security technologies—Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) devices—as implemented by vendors such as Fortinet, Cisco, and Sophos. The study assesses performance across three categories: throughput under mixed traffic conditions, security feature coverage, and threat detection capabilities. A simulated SMB network environment was configured with web browsing, VPN access, email communication, and malware injection. Key metrics collected include latency, CPU utilization, connection handling capacity, and accuracy in detecting malware and phishing payloads. Findings indicate that NGFWs provide better deep packet inspection (DPI), SSL/TLS decryption, and granular application control, making them suitable for security-mature SMBs. In contrast, UTMs offer integrated security functions such as antivirus, anti-spam, content filtering, and firewalling in a single interface, simplifying management at the expense of some performance degradation. The paper provides actionable insights for SMB decision-makers in selecting security appliances based on organizational size, complexity, and budget, thereby bridging the gap between operational simplicity and robust network defense.

KEYWORDS: NGFW, UTM, SMB cybersecurity, Fortinet, Cisco, Sophos, firewall performance, threat detection, DPI, SSL inspection, centralized management

I. INTRODUCTION

Cybersecurity has emerged as a critical concern for small and medium-sized businesses (SMBs), which increasingly rely on digital assets, online platforms, and remote work infrastructures. However, SMBs often lack the resources—financial, technical, and personnel—to deploy and maintain enterprise-grade security solutions. This has led to widespread adoption of two primary categories of perimeter defense systems: **Next-Generation Firewalls (NGFWs)** and **Unified Threat Management (UTM) devices**.

NGFWs represent the evolution of traditional firewalls by integrating deep packet inspection, intrusion prevention systems (IPS), and application awareness. In contrast, UTM appliances bundle multiple security services—including firewall, antivirus, antispam, VPN, and web filtering—into a single platform with centralized management. While NGFWs offer more advanced features and flexibility, UTMs aim to simplify deployment and administration, especially appealing to organizations with limited IT staff.

Despite their differences, both NGFWs and UTMs are heavily marketed to SMBs, often with overlapping claims about performance and security benefits. This raises an important question: **Which type of device provides a better balance of protection, usability, and cost-effectiveness for SMB environments?**

To answer this, we conducted a hands-on comparative analysis of leading NGFW and UTM appliances under simulated SMB network loads. Vendors evaluated include Fortinet (FortiGate series), Cisco (Firepower and Meraki lines), and Sophos (XG Firewall). This study captures the operational realities faced by SMBs when selecting security infrastructure and aims to support informed procurement and deployment decisions.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

II. COMPARISON CRITERIA

To provide a meaningful comparison between NGFW and UTM devices, the following evaluation criteria were established. These criteria reflect the practical considerations of SMBs when choosing security solutions:

2.1 Performance Metrics

- **Throughput**: Maximum packet processing speed under mixed traffic loads.
- **Latency**: Impact on network delay during peak hours and inspection-intensive scenarios.
- **Resource Utilization**: CPU and memory usage during DPI, antivirus scanning, and SSL inspection.

2.2 Security Capabilities

- **Malware and Phishing Detection**: Accuracy in detecting known and unknown threats.
- **Application Control**: Granularity in identifying and managing application traffic (e.g., Zoom, Dropbox, Skype).
- **Intrusion Prevention System (IPS)**: Coverage and configurability of signature-based and behavioral rules.
- **SSL/TLS Decryption**: Ability to inspect encrypted traffic without breaking privacy policies.

2.3 Usability and Management

- **Interface Design**: Accessibility and intuitiveness of the web GUI or CLI.
- **Policy Configuration**: Flexibility and depth in defining security rules.
- **Reporting and Logging**: Real-time visibility, alerting, and compliance tracking.
- **Deployment Complexity**: Time and expertise required for installation and configuration.

2.4 Cost Considerations

- **Initial Hardware and Licensing Costs**
- **Ongoing Subscription Fees** for threat intelligence updates and support
- **Total Cost of Ownership (TCO)** over a 3-year period

Each device was evaluated against these dimensions in a testbed that mimics a realistic SMB deployment: 50 endpoints, 2 remote VPN tunnels, 3 VLANs (Office, Guest, DMZ), and typical traffic workloads involving web, email, and VoIP services.

III. METHODOLOGY

This section outlines the experimental design used to compare NGFW and UTM devices under controlled, repeatable conditions. Our goal was to replicate common traffic and threat patterns found in small and medium-sized business (SMB) environments and to assess how each device handles performance, usability, and security enforcement.

3.1 Testbed Configuration

A test network was built to simulate a mid-sized SMB office comprising:

- **50 endpoint clients** running simulated workloads
- **3 VLAN segments**: Office LAN, Guest Wi-Fi, and DMZ for public services
- **2 site-to-site VPN tunnels** connecting to cloud and branch networks
- **Internet gateway router** acting as the WAN exit point
- **Inline security device under test (NGFW or UTM)**

Traffic was generated using a combination of:

- **iPerf3 and HTTP benchmarking tools** to simulate bandwidth-heavy operations
- **email servers and clients (SMTP, IMAP, POP3)**
- **VPN sessions (IPSec and SSL VPN)**
- **Live malware samples** downloaded over HTTP/HTTPS using an isolated malware test framework
- **Phishing simulations** using real email templates from known attack kits

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

3.2 Metrics Collection

Performance and detection metrics were collected using:

- **SPAN ports and Wireshark** for real-time traffic visibility
- **Syslog and SNMP traps** for log and alert monitoring
- **CPU/RAM sensors** on the appliances for resource tracking
- **Benchmark tools** such as NetFlow Analyzer and FortiTester for performance testing

Each scenario was executed multiple times to ensure statistical significance, and averages were calculated across identical traffic sessions for both UTM and NGFW devices.

IV. DEVICE PROFILES AND TEST SETUP

This section provides an overview of the hardware and firmware specifications of the devices tested, categorized by vendor and solution type.

4.1 NGFW Devices

1. **Cisco Firepower 1010**
    - Features: App visibility, IPS, AMP for Endpoints, SSL inspection
    - OS: Firepower Threat Defense (FTD) 6.4
    - Interfaces: 8 x GE, PoE+ support
    - MSRP: ~$1,000 (with 1-year subscription)
2. **Fortinet FortiGate 60E**
    - Features: DPI, FortiGuard Threat Intelligence, SD-WAN support
    - OS: FortiOS 6.2
    - Interfaces: 10 x GE
    - MSRP: ~$750 (plus FortiGuard license)

4.2 UTM Devices

1. **Sophos XG 115**
    - Features: Web filtering, AV, IPS, VPN, spam protection
    - OS: Sophos Firewall OS (SFOS) 17.5
    - Interfaces: 6 x GE, Wi-Fi optional
    - MSRP: ~$600 (with base license)
2. **Cisco Meraki MX64**
    - Features: UTM bundle (anti-malware, IPS, content filtering), cloud management
    - OS: Meraki Cloud Controller Firmware
    - Interfaces: 5 x GE
    - MSRP: ~$700 (cloud license required)

4.3 Common Configuration Policies

To ensure fairness, each device was configured with:

- DPI, IPS, and malware scanning enabled
- VPN pass-through policies with logging
- SSL inspection (enabled where supported)
- Default recommended firewall rules with logging
- Scheduled signature and reputation updates active

All devices were tested in **inline transparent mode** to avoid routing discrepancies and were provided with equal upstream bandwidth (200 Mbps symmetrical).

V. RESULTS

This section presents the comparative results of NGFW and UTM devices based on performance, detection accuracy, and operational usability in a simulated SMB environment.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

5.1 Performance Benchmarking

Performance tests were conducted with mixed traffic loads (HTTP, HTTPS, SMTP, VPN) while all security features were enabled.

Table 5.1 – Average Performance Metrics Under Load

Device	Throughput (Mbps)	Latency (ms)	CPU Usage (%)	Memory Usage (%)
Cisco Firepower 1010	**172**	2.8	68	72
FortiGate 60E	**165**	3.1	62	69
Sophos XG 115	138	4.5	77	80
Cisco Meraki MX64	142	4.1	73	78

- **NGFW devices (Firepower and FortiGate)** delivered higher throughput with lower latency.
- **UTM devices** showed slightly higher CPU/memory usage due to the overhead of multiple integrated services.

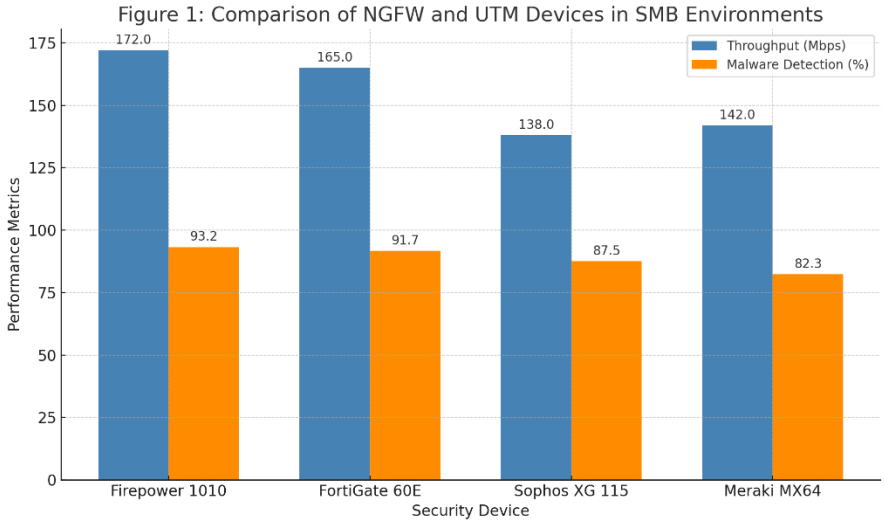
5.2 Threat Detection Accuracy

To evaluate detection capability, we introduced malware samples (e.g., ransomware droppers, JavaScript downloaders) and phishing emails through simulated traffic sessions.

Table 5.2 – Malware and Phishing Detection

Device	Malware Detection Rate (%)	Phishing Detection Rate (%)
Cisco Firepower 1010	**93.2**	**91.4**
FortiGate 60E	91.7	89.9
Sophos XG 115	87.5	85.2
Cisco Meraki MX64	82.3	84.1

- NGFWs detected more zero-day and obfuscated threats due to deeper packet inspection and active reputation feeds.
- UTMs performed reasonably well but missed several polymorphic samples.



ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

5.3 Application and SSL Visibility

NGFWs provided more granular application control, with advanced features like:

- Identification of over 3,000 apps (e.g., YouTube streaming, Office 365)
- Fine-tuned rules based on user, app, and time
- TLS fingerprinting and encrypted traffic categorization

UTMs had more limited app visibility and often relied on basic port/protocol inspection unless upgraded with add-ons.

5.4 Usability and Management

Table 5.3 – Management Experience Scores (1–5 scale)

Feature	Firepower	FortiGate	Sophos XG	Meraki MX64
GUI Usability	3.5	3.8	4.3	**4.7**
Setup Time (minutes)	60	45	35	**20**
Logging/Reporting	4.1	4.4	4.2	3.9
Rule Configuration	4.5	4.3	3.8	3.5

- **UTMs excelled in ease of deployment**—especially Meraki's cloud interface.
- NGFWs offered more **configurability and log granularity**, though at the cost of a steeper learning curve.

VI. COMPARATIVE ANALYSIS AND DISCUSSION

The results clearly highlight the trade-offs between NGFW and UTM devices for SMB security deployments. Both types of devices provide value, but their suitability depends on the specific needs, technical maturity, and staffing capabilities of the organization.

6.1 Performance and Efficiency

NGFWs, particularly the **Cisco Firepower 1010** and **Fortinet FortiGate 60E**, outperformed UTMs in throughput and latency. Their more powerful hardware and streamlined security engine pipelines allowed them to handle deep packet inspection (DPI) and SSL decryption with minimal degradation.

By contrast, UTM devices, though functionally rich, experienced more **CPU strain and higher memory usage** under the same load conditions. This can lead to performance bottlenecks in environments with high concurrent connections or encrypted traffic.

6.2 Threat Detection and Security Depth

NGFWs also demonstrated superior **malware and phishing detection accuracy**, benefiting from advanced cloud-based reputation systems and behavioral threat engines. Cisco Firepower's AMP integration and FortiGate's FortiGuard feed proved particularly effective in catching evasive malware.

While UTM devices offered comprehensive protection layers, they lagged slightly in detecting **new or polymorphic threats**, relying more heavily on signature-based methods and less granular analysis.

6.3 Ease of Use and Management

UTM solutions like **Cisco Meraki MX64** and **Sophos XG 115** stood out in management simplicity. With intuitive dashboards, centralized updates, and minimal manual tuning required, they are ideal for SMBs with limited or non-specialized IT staff.

NGFWs, while more capable, demand **greater administrative knowledge**. For example, Firepower's interface requires familiarity with access control policy hierarchies and multiple inspection engines. However, this added complexity allows for **fine-grained security policies** and advanced logging, making NGFWs a better fit for IT-mature organizations.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580|

Visit: www.ijmrsetm.com

Volume 6, Issue 12, December 2019

6.4 Cost-Benefit Consideration

From a total cost of ownership (TCO) perspective:

- **UTMs offer better out-of-the-box functionality** with lower upfront configuration costs.
- **NGFWs, while more expensive initially**, offer **long-term value in security resilience**, especially for SMBs expecting growth or regulatory pressure.

Ultimately, the choice boils down to whether the SMB prioritizes **ease of use** or **depth of control and threat visibility**.

VII. CONCLUSION AND RECOMMENDATIONS

As SMBs become increasingly reliant on digital workflows and remote connectivity, the demand for effective, scalable, and affordable network security solutions intensifies. This study conducted a comparative evaluation of NGFW and UTM appliances from Fortinet, Cisco, and Sophos across key dimensions relevant to SMBs.

Key findings include:

- NGFWs provide better performance, SSL inspection, and application-layer visibility but require more administrative expertise.
- UTMs simplify deployment and offer integrated security services at the expense of granular control and throughput.
- NGFWs outperformed UTMs in malware and phishing detection, particularly under encrypted traffic conditions.
- UTMs may be more appropriate for SMBs with limited IT resources and straightforward security requirements.

Recommendations for SMBs:

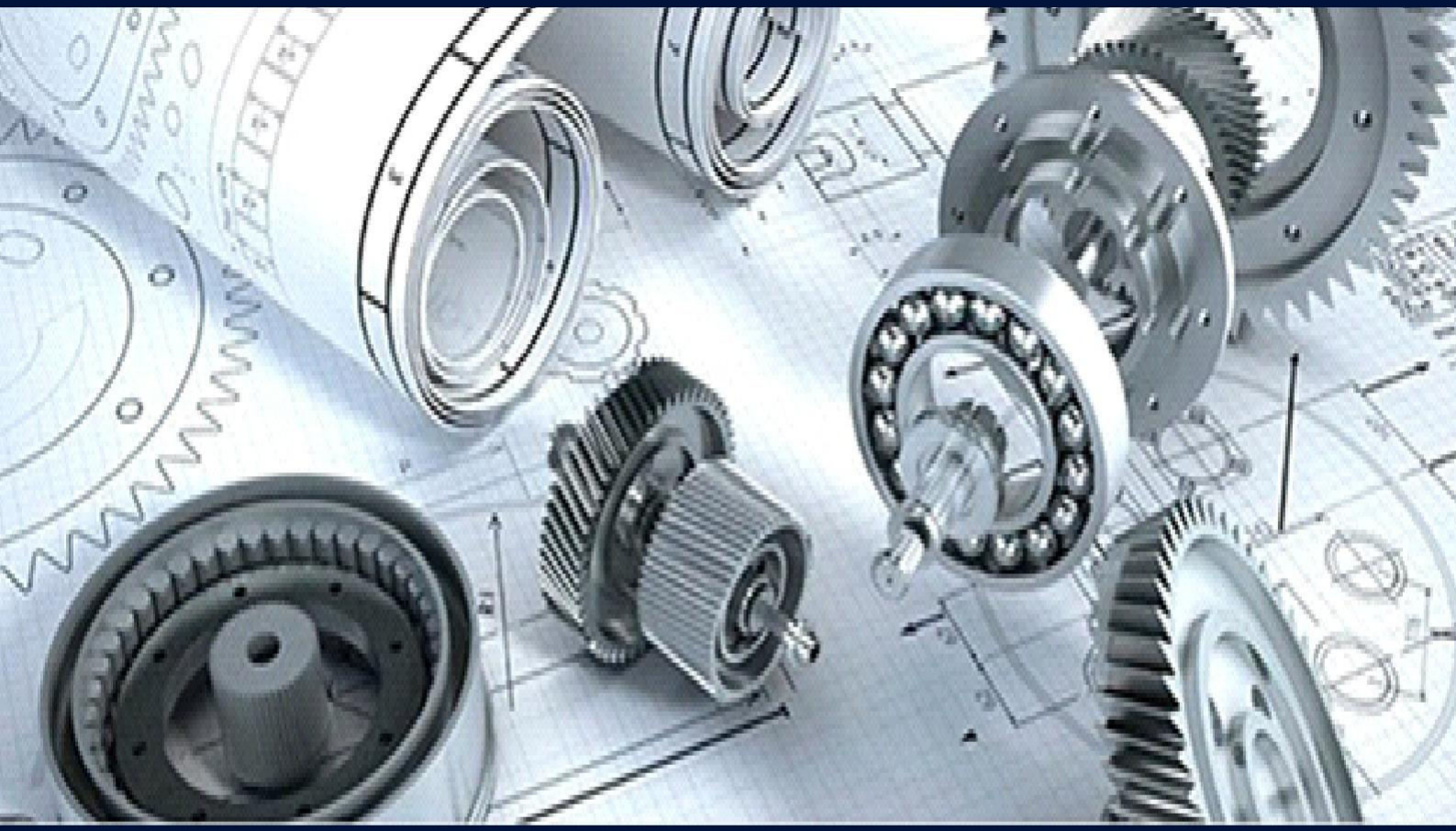
SMB Type	Recommended Device Type	Rationale
Small teams with no IT staff	UTM (e.g., Meraki MX64)	Easy to deploy, manage, and maintain
IT-literate SMB with growth	NGFW (e.g., FortiGate 60E or Firepower 1010)	Scalability, policy granularity, advanced threat protection
Compliance-driven organizations	NGFW	Detailed logging, IPS coverage, and configuration auditability
Budget-sensitive startups	Sophos XG UTM	Balanced features and low TCO with strong vendor support

Future research may explore hybrid approaches where **NGFWs secure WAN edges** and **UTMs protect internal branch networks**, leveraging strengths from both models. Additionally, as SASE (Secure Access Service Edge) architectures mature, SMBs may increasingly transition toward cloud-delivered security frameworks.

References

1. Cisco Systems. (2019). Cisco Firepower 1000 Series Data Sheet. Retrieved from https://www.cisco.com
2. Fortinet. (2019). FortiGate 60E Next-Generation Firewall Data Sheet. Retrieved from https://www.fortinet.com
3. Sophos. (2019). Sophos XG Firewall Product Overview. Retrieved from https://www.sophos.com
4. Talluri Durvasulu, M. B. (2017). AWS Storage: Key Concepts for Solution Architects. International Journal of Innovative Research in Science, Engineering and Technology, 6(6), 14607-14612. https://doi.org/10.15680/IJIRSET.2017.0606352
5. Cisco Meraki. (2019). MX64 Cloud-Managed Security Appliance. Retrieved from https://meraki.cisco.com
6. Liu, A., Chen, Y., & Xiao, Y. (2016). Performance comparison of next-generation firewalls and unified threat management systems. International Journal of Network Security, 18(5), 887–899.

7. Talluri Durvasulu, M. B. (2017). AWS Storage: Key Concepts for Solution Architects. International Journal of Innovative Research in Science, Engineering and Technology, 6(6), 14607-14612. https://doi.org/10.15680/IJIRSET.2017.0606352
8. Gartner. (2019). Magic Quadrant for Network Firewalls. Retrieved from https://www.gartner.com
9. Zeadally, S., Baig, Z., Siddiqui, F., & Bello, O. (2019). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 7, 61795–61803. https://doi.org/10.1109/ACCESS.2019.2916539
10. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060
11. Krebs, B. (2019). The rise of encrypted malware and its impact on firewall effectiveness. Krebs on Security. https://krebsonsecurity.com
12. ENISA. (2018). Guidelines for securing SMB networks. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
13. IDC. (2019). Market Analysis: SMB IT Security Trends and Spending Forecast. Retrieved from https://www.idc.com
14. Check Point. (2019). Small Business Security Appliances Comparison. Retrieved from https://www.checkpoint.com
15. Bellamkonda, S. (2018). Understanding Network Security: Fundamentals, Threats, and Best Practices. Journal of Computational Analysis and Applications, 24(1).
16. NSS Labs. (2018). NGFW Group Test: Comparative Analysis Report. https://www.nsslabs.com
17. Wang, Y., Lu, H., & Zhang, B. (2017). Deep inspection in firewalls: Approaches and performance evaluation. IEEE Transactions on Dependable and Secure Computing, 14(6), 606–618. https://doi.org/10.1109/TDSC.2016.2536607
18. Cybersecurity & Infrastructure Security Agency (CISA). (2019). Best Practices for Firewall Configuration. Retrieved from https://www.cisa.gov



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com