# Multi-Layered Protection against Ransomware Attacks Using Moving Target Defense (MTD) Strategy

Snehal R. Shinde[1], Dr. Jagdish W. Bakal[2]
[1]*PhD Schlor, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra, India*
[2]Principal, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra, India

**Abstract**
The prevalence and sophistication of ransomware attacks have surged in recent years, presenting formidable threats to critical infrastructure sectors. This alarming evolution necessitates a robust, adaptive security approach. Traditional single-layer defenses are increasingly insufficient against advanced adversarial tactics, including polymorphic malware and zero-day exploits. To address this escalating threat, a multilayer defense architecture is imperative to strengthen protection across endpoints and networks. Rather than relying on static configurations, Moving Target Defense (MTD) enhances protection by introducing dynamic variability into the cyber environment, thereby interrupting attacker reconnaissance and exploitation. In this paper, a multi-layered defense strategy is developed against ransomware attacks leveraging MTD. The methodology integrates MTD within endpoint protection, firewall security, and execution control layers to create a robust and adaptive security posture. The proposed approach continuously mutates access policies, rotates network addresses, and shuffles execution policies to reduce attack surface and thwart reconnaissance efforts. This layered defense framework ensures that ransomware attempts can be interrupted at multiple layers, thereby substantially lowering the probability of a successful breach. The result proved the effectiveness of the proposed approach in protecting the system against ransomware attacks in terms of IP rotation, execution token shuffling, policy mutation variability, probability of compromise, and attack risk.

***Keywords:*** **Cyberthreat; Ransomware; Security; Multi-layered defense; Moving Target Defense**

## 1. Introduction

The unprecedented expansion of digital technologies and ubiquitous data connectivity has dramatically widened the landscape of cyberattacks, with ransomware emerging as one of the disruptive forms of cyber threats worldwide [1]. Ransomware is a rapidly evolving malware engineered for encrypting files on electronic devices, rendering them inaccessible until a ransom is paid. The escalating sophistication of ransomware attacks is fuelled by increasingly sophisticated threat vectors employing multidimensional transformations, significantly complicating detection and prevention [2]. Malicious actors leverage advanced technologies, including obfuscation and polymorphic encryption, to evade modern antimalware defenses. The proliferation of zero-day attacks further exacerbates early detection, allowing ransomware to encrypt files before security measures can effectively respond. Moreover, the utilization of anonymous financial channels, such as cryptocurrencies and peer-to-peer payment systems, enables attackers with an untraceable medium for extortion, making ransomware more resilient and difficult to counter [3]. It predominantly manifests in two variants: Crypto Ransomware that encrypts critical files and demands payment from victims for decryption. The Locker Ransomware locks users' access to their operating system, requiring payment to restore functionality [4]. Ransomware remains a highly adaptive and evolving cybersecurity threat, continuously refining its attack methods to maximize impact. Hence, countermeasures must evolve in tandem, as solutions effective against one variant may prove obsolete against newer variants. Therefore, the development of broad-spectrum detection and prevention strategies is imperative, emphasizing early threat identification, robust security mechanisms, and secure backup solutions for mitigating financial and operational risks [5].

The increasing prevalence of ransomware attacks necessitates the adoption of a comprehensive, multi-layered security strategy, ensuring robust organizational defense. A multi-layered approach combines diverse protective mechanisms, acknowledging that no single security solution can offer complete protection against evolving ransomware threats [6]. By implementing multiple defense layers, organizations can proactively detect and neutralize potential ransomware infections before they execute encryption routines or propagate laterally across networks, to ensure a robust and resilient defense. However, conventional multilayer defense mechanisms are inadequate against ransomware due to their inherently static architecture, enabling attackers to systematically analyse and bypass security measures over time. Security implementation gaps create exploitable attack vectors, while delayed patching—often stemming from concerns over service quality— further exacerbate system vulnerabilities. Furthermore, zero-day attacks targeting unknown

vulnerabilities can render conventional defense mechanisms ineffective, providing ransomware ample opportunity to infiltrate critical infrastructures and execute malicious payloads unimpeded [7].

To mitigate these constraints, Moving Target Defense (MTD) has arisen as a proactive security paradigm for counteracting adaptive adversaries through the continuous modification of system configurations, such as network settings, open network ports, and software components. By introducing persistent variability, this dynamic strategy increases uncertainty for attackers, thus efficiently reducing the advantage derived through reconnaissance and rendering traditional attack methods increasingly obsolete [8][9]. MTD loses its efficiency when the shifting mechanism follows a predictable pattern, since adversaries can eventually decipher and adapt their attack strategies accordingly. To sustain resilience, MTD must integrate randomness, ensuring that system adaptations remain resistant to anticipation [10].

The average ransom demanded by attackers surged by 500% over a year, escalating to a staggering mean payment of $2 million [11]. Hence, combining MTD with a multi-layered defense architecture enhances ransomware protection by dynamically modifying system configurations, thus complicating vulnerability exploitation. MTD effectively thwarts reconnaissance efforts, while multi-layered security reinforces anomaly detection, strict access controls, and real-time threat mitigation. This synergistic integration minimizes the attack surfaces and avoids lateral movement within networks. By leveraging deception mechanisms, dynamic access control, and proactive recovery mechanisms, this unified approach strengthens system resilience. Collectively, MTD and multi-layered defenses provide a robust, adaptive security infrastructure, capable of protecting the system against the persistent evolution of ransomware threats.

The contributions of the proposed work are:

- To develop a robust and adaptive MTD-enabled multilayer defense framework that integrates seamlessly across endpoint protection, firewall security, and execution control layers.
- To effectively hinder attacker reconnaissance and exploitation efforts, it continuously mutates access policies, rotates network addresses, and shuffles execution policies to reduce the attack surface.
- To implement and validate the effectiveness of the proposed approach in terms of IP rotation variability (IRV), execution token shuffling variability (ETSV), policy mutation variability (PMV), probability of compromise (PoC), and attack risk (AR).

### 1.1 Paper Organization

The subsequent sections of this paper are organized as follows: In Section 2, relevant literature is discussed and compared to identify the research gaps. Section 3 delineates the preliminaries of ransomware attacks, multilayer defense, and MTD. Section 4 encompasses discussions on the attack model, problem formulation, and proposed methodology. Section 5 elucidates the results obtained, while Section 6 provides conclusions.

## 2. Literature Review

Existing works that explore multilayer defense strategies and MTD strategies for defense against evolving attack trends are discussed in detail.

### 2.1 Previous Works Related to Multilayer Defense Mechanisms

Conventional antivirus and antimalware solutions are insufficient in mitigating ransomware attacks, as human error remains the predominant attack vector. A multi-layered defense approach [12] is imperative, integrating advanced antimalware defenses, firewalls, domain name system (DNS)/Web filtering, email security, data backups, and targeted employee awareness training. Properly implemented layered defense strategies intercept ransomware at multiple attack stages, minimizing the probability of infection. However, empirical evidence from real-world deployments remains limited. An SDN-based defense mechanism [13] is proposed that utilizes Rényi entropy for fine-grained traffic analysis. It enhances response speed and attack detection accuracy by improving computational efficiency. However, the defense mechanism did not have optimal real-time response capabilities. A strategy in [14] is proposed for strengthening energy infrastructure cybersecurity via organizational, technical, and policy-driven measures. Even though it prioritizes human factor vulnerabilities, technical cyberattacks like advanced persistent threats, zero-day exploits, and ransomware need advanced dynamic countermeasures.

Existing multilayer defense approaches, particularly developed for defense against ransomware, are discussed. A four-layered defense architecture [6] is proposed that involves policies, recursive folder, process monitoring, and backup & recovery for detecting and preventing ransomware execution. It safeguards systems by preventing encryption, blocking infiltration, observing processes, and ensuring data recovery. By identifying short-term and long-term behavioural anomalies, a multilayer temporal anomaly patterns (ML-TAP) framework [15] is proposed for ransomware detection. Unlike conventional signature-based techniques, it autonomously fine-tunes detection criteria by iterative analysis of high-dimensional data streams, to ensure adaptability against polymorphic attacks. Lightweight intrusion detection system (L-IDS) [16] integrates multilayer controls and a TrustZone-based trusted execution environment (TEE) for improved security. L-IDS efficiently detects and alleviates ransomware in resource-constrained IoT systems with less computational overhead.

### 2.2 Previous Works Related to Moving Target Defense Mechanisms

Existing defenses often become obsolete when attackers adapt, requiring the development of more resilient security frameworks. An MTD-based Trojaning attack defense framework is proposed in [17] through a signalling game model. MTD improves attack costs, thereby strengthening security against Trojaning attacks, ensuring model availability while mitigating emerging threats. To address the intricate nature of IoT connectivity and device vulnerabilities, a proactive defense framework is proposed [18] that integrates MTD and cyber deception. Decoy nodes are utilized for deception and OS diversity, altering the attack surface and minimizing threats. An important measure-based OS diversity technique reduces defense cost. Although OS diversity increases the effort and cost for the attacker, it does not essentially lessen the risk to the system. A security framework is proposed in [19] for IoT devices in cloud environments. It protects against false data injection and DDoS attacks using simple network management protocol (SNMP), Kullback–Leibler distance (KLD), access control rules (ACL), and MTD techniques. While SNMP and KLD detect threats, ACL and MTD alleviate attacks by minimizing the attack surface, thus reducing the attack probabilities and delays. The study does not address other IoT threats such as side-channel attacks, ransomware, or firmware exploits.

Despite MTD's effectiveness, research on hybrid MTD techniques remains limited, particularly in optimizing cost, efficiency, and security trade-offs in IoT systems. MTD results in resource overutilization, motivating the development of a three-layer Temporal Hierarchical Attack Representation Model (3-layer-THARM) [20] for vulnerability defense. Combining MTD techniques such as shuffle and diversity enhances security by improving attack costs and minimizing attack success rates and risks. However, MTD leads to more resource consumption and interrupts network services. MTD mechanism in [21] utilizes the dynamic host configuration protocol for enabling IP-Hopping. It prevents malicious attacks in industrial and medical environments. Depending on DNS lookup, problems such as time synchronization and IP conflicts are avoided with reduced large-scale deployment costs.

Four MTD mechanisms are proposed in [22] that dynamically adapt data, network, and runtime environments for mitigating malware. A lightweight IoT-oriented MTD framework is implemented in real-world situations. However, the decision-making process mainly depends on predefined rules that may not adapt well to evolving malware variants. MTD-enabled file system (MTFS) is introduced in [23] that utilizes trapping recursive directory traversal, delaying attackers, and hiding file types. The system functions with less resource overhead, representing its possibility for proactive defense. As MTFS depends on FUSE for file operations in user space, it may incur more performance overhead than kernel-level implementations. A novel MTD framework [24] is proposed for Windows to tackle data theft ransomware attacks. MTD improves security by dynamically modifying system configurations, complicating attack execution. However, the requirement for further optimization of MTD activation triggers balancing ransomware defense and inducing service disruption. An MTD approach [25] is proposed for preventing ransomware encryption by modifying the attack surface. The first defense layer hides known file extensions for protecting against targeted encryption, whereas the second layer utilizes event-driven MTD for dynamically changing file extensions upon the detection of ransomware-like activities. These approaches reduce the attack success ratio and protect user information. The method in [26] is developed to optimize MTD selection against zero-day attacks in single-board computers. It learns effective MTD approaches through behavioural fingerprinting. However, it struggles to counter passive malware that does not show overt malicious behavior. Table 1 shows the comparison of the existing security approaches related to ransomware.

Table 1. Comparison of the Existing Security Approaches Related to Ransomware

| Author (year) [ref] | Objectives | Attack Model | Security Measures | Contributions | Limitations |
|---|---|---|---|---|---|
| Pagán and Elleithy (2021) [12] | Multi-layered defense to safeguard against ransomware | Ransomware | Multi-layered defense | Interrupts ransomware at several stages, minimizing infection probability and allowing secure backups for data recovery | There is no empirical validation from real-world deployments. |
| Ryu et al. (2024) [14] | Enhancing cybersecurity through a layered defense approach | Malware | Layered defense | Reinforces energy infrastructure cybersecurity via network segmentation, anomaly detection, and system integrity checks | Did not sufficiently address zero-day exploits and ransomware |

| | | | | | |
|---|---|---|---|---|---|
| Denis et al. (2024) [15] | Autonomous ransomware detection using multilayer temporal anomaly patterns | Ransomware | Layered temporal analysis | Identifies short-term and long-term behavioural anomalies, facilitating adaptive detection of polymorphic ransomware | Difficulty in achieving computational efficiency in real-time high-dimensional data analysis |
| Mofidi et al. (2024) [16] | Multi-layered approach to ransomware detection | Ransomware | Multi-layered defense | Utilizes multilayer controls, TrustZone-based TEE for efficient ransomware detection in IoT | May not be scalable to large-scale IoT networks with different security demands |
| Assen et al. (2022) [22] | Lightweight MTD framework for multi-purpose malware | Malware: Botnet, Ransomware, Rootkit, Backdoor | MTD | Dynamically alters network and data for mitigating IoT malware threats | Depends on predefined rules, difficult for adaptive to malware variants |
| Assen et al. (2023) [23] | MTD-enabled file system for malware mitigation | Malware: ransomware | MTD | Utilizes trapping, delaying, and hiding file types with reduced resource overhead | FUSE-based user-space implementation may introduce performance overhead. |
| Khan et al. (2022) [25] | Ransomware prevention using MTD | Ransomware | MTD | Dynamically modifies file extensions to reduce ransomware attack success rate. | May not be effective against ransomware variants that do not depend on file extensions for encryption targeting. |
| Celdr´an et al. (2022) [26] | MTD for Zero-day Attacks | Ransomware | MTD | Learns effective MTD mechanisms using behavioural fingerprinting | Difficulty in mitigating passive malware that does not show overt malicious behavior |

In spite of significant efforts in ransomware defense, existing solutions reveal critical gaps that motivated the development of the proposed multi-layered MTD strategy. Studies [12][14] highlight layered defense approaches but fall short in handling real-world ransomware incidents, particularly zero-day variants, due to the absence of empirical validation and insufficient adaptability. Moreover, they consider static multilayer defense mechanisms, which depend on fixed configurations, predefined rules, and rigid access controls, struggle to cope with the evolving tactics of ransomware adversaries. While MTD-based frameworks [22][23][25] introduced dynamic file and network manipulation, they often depend on predefined rules or were narrowly focused, limiting efficacy against evolving ransomware tactics. Additionally, the study in [26] struggles to detect passive ransomware that avoids overt behaviour. Most existing studies either concentrate solely on MTD or implement static multilayer defenses without dynamic adaptation strategies. None of the existing works effectively combine MTD with a comprehensive multi-layered defense strategy against ransomware.

## 3. Preliminaries

The basic concepts related to ransomware, multilayer defense systems, and MTD are given below.

### 3.1 Ransomware

Ransomware attacks exploit asymmetric encryption for targeting systems, adhering to a structured workflow comprising four phases. During *Delivery and Reconnaissance,* attackers collect information about the target such as network infrastructure, IP addresses, and system vulnerabilities, to identify possible exploitation paths. Several infection vectors are utilized for penetrating systems, such as zero-day exploits, phishing emails, security vulnerabilities, malicious mobile media, compromised software supply chains, and remote desktop protocol breaches. Moreover, sophisticated methods, including exploit kits, self-propagation mechanisms, and obfuscation techniques, aid ransomware in avoiding conventional antivirus detection. During the *Attack Instruction phase*, ransomware deploys itself using malicious files, DLLs, and stealth techniques upon infiltration to evade detection systems. It subsequently propagates laterally across the

network through file-sharing protocols and other communication channels to maximize its impact while maintaining persistence within the compromised environment. During the *Destruction phase*, the ransomware executes its malicious code, systematically encrypting valuable files, such as documents, databases, and multimedia files. In certain scenarios, it may exploit security vulnerabilities to spread into interconnected infrastructures, intensifying its destructive potential. During the *Extortion Demand phase*, attackers demand a ransom after successful encryption, threatening permanent data loss or system failure when payment is not made. However, even when the ransom is paid, there is no assurance that the decryption key offered will successfully restore the data, leaving victims susceptible to both financial loss and permanent file corruption [27].

### 3.2 Multilayer Defense System

A multi-layered ransomware defense strategy includes several layers, each concentrating on diverse aspects of cybersecurity for ensuring comprehensive protection against ransomware. The key layers are discussed as follows. *Endpoint Protection* layer safeguards user devices against ransomware and malware attacks. As conventional antivirus software is inadequate, modern endpoint protection solutions must integrate process tracking, behavioural monitoring, and endpoint isolation for detecting threats at an early stage. *Firewall Security* layer acts as the first network defense that filters outbound and inbound traffic depending on pre-determined rules. A well-configured firewall must block identified malicious ports, implement geolocation restrictions, and keep updated allow/block IP lists. By filtering out unsafe DNS requests, *the DNS/Web Filtering* layer prevents users from accessing malicious websites. Moreover, this layer improves security by blocking those websites depending on categories, such as phishing and malware, and supporting whitelisting and blacklisting of particular domains. *Data Backup and Recovery* layer ensures steady and secure backups for preventing data loss during a ransomware attack. Onsite backups must be kept in a distinct subdomain with one-way trust, thereby ensuring adversaries cannot access backup credentials even when they penetrate the main domain. Offsite backups in cloud or physical servers are reliable when compared to onsite backup exploitation. The *Email Security* layer includes email filtering and security gateways to protect the system against malware attachments, phishing, and fake emails. It enables more granular filtering by finding suspicious senders and blocking malicious file extensions without blocking entire domains. *The execution control* layer controls process execution depending on security policies, user privileges, and behavioural analysis for preventing malicious or unauthorized code execution. By implementing these multiple layers, organizations can develop a robust ransomware defense to protect the system while minimizing the risk of successful attacks [6][12].

### 3.3 Moving Target Defense

**Definition:** MTD allows us to create, analyse, evaluate, and deploy mechanisms and strategies that are different and that continually change over time, increasing the complexity and cost for attackers, limiting the exposure of vulnerabilities and possibilities for attack, and increasing the system resiliency [28].

MTD is a cybersecurity strategy intended to improve network security through dynamism and uncertainty in system configurations. Conventional static defenses facilitate attackers to progressively enhance their knowledge of the system over time, exploit vulnerabilities, and establish obstinate attack paths. The predictability and homogeneity of traditional networks make them more vulnerable to attacks with minimized costs and improved benefits for adversaries. MTD alleviates this risk by continuously changing the attack surface, while minimizing reconnaissance effectiveness and restricting the window of opportunity for attacks. MTD increases attack complexity and difficulty by dynamically modifying configurations, including operating systems, network protocols, or service endpoints.

Based on the attack surface, MTD theory concentrates on minimizing vulnerabilities in network systems by dynamically modifying system configurations. The attack surface includes communication channels, entry methods, and untrusted information. Attack surface changes happen when system vulnerabilities vary, affecting an attacker's capability to exploit them. Moving attack surfaces lead to uncertainty, thereby enhancing security through configuration diversity and restricted exposure time. On the basis of system vulnerabilities, attack goals, and connectivity, attack graphs model exploit sequences. MTD modifies attack graphs by altering network configurations and interrupting an attacker’s path. MTD theory highlights defense strategies that increase attack complexity with improved system performance, in which attack graph-based analysis aids in evaluating its efficiency in mitigating cyber-attacks.

The concepts of MTD design depend on three vital questions: What to Move that identifies the system components that vary over time (network configurations, protocols, or other system attributes); When to Move that defines the timing of state variations (either fixed, random, or event-driven); and How to Move that determines the technique of transition between states, guided by probability distributions, game theory, or fixed sequences.

Its design principles concentrate on unpredictability, coverage, and timeliness. Coverage guarantees that MTD dynamically alters a significant portion of vulnerabilities, whereas unpredictability upsurges the uncertainty of attackers, making it difficult to exploit weaknesses. Timeliness ensures that MTD triggers before an attack happens, thereby preventing exploitation. Additional principles comprise assuring system

availability, utilizing natural and artificial diversity, and applying moving, distinguishable features for differentiating between benign users and attackers. MTD architectures progress from proactive to reactive defense and then into adaptive systems. Proactive defense architectures depend on predefined tactics and random transformations but fail due to inefficiencies. Reactive defense architectures combine logic security models and analysis engines for targeted defense. Advanced architectures integrate task awareness for adaptable deployments and a man-machine relationship to enhance strategy formulation through expert knowledge. The evolution from manual to hybrid automation improves MTD effectiveness while ensuring adaptive and effective defense deployment [8].

## 4. Proposed Methodology

### 4.1 Attack Model

Attacker is assumed to be a highly adaptive ransomware actor who can execute multi-phase attacks targeting the integrity, confidentiality, and availability of critical assets. The attack starts with reconnaissance for identifying static system configurations such as fixed execution privileges, access control rules, and network IP assignments. By utilizing stolen or escalated credentials, the attacker infiltrates the system, bypasses the endpoint defenses, and obtains privileged access to sensitive processes and files. After entering the system, the attacker tries to execute malicious code by manipulating predictable execution control policies and process whitelists. Simultaneously, exposed or unmapped IP addresses in the internal network are targeted to spread laterally, maximizing the infection spread before detection. Additionally, the attacker observes policy patterns over time for anticipating and exploiting static access control rules, particularly targeting critical user access to sensitive files. The main goal of the attacker is to encrypt critical files, interrupt system operations, and request ransom payments, while evading detection by exploiting the predictability of fixed security parameters.

### 4.2 Problem Formulation

The problem of designing a multilayer defense strategy for protection against ransomware attacks using MTD can be formulated as an optimization problem. Assume that the system has N users, which is denoted as $U = \{u_1, u_2, ..., u_N\}$, with M files, denoted by $F = \{f_1, f_2, ..., f_M\}$. $P = \{p_1, p_2, ..., p_s\}$ is the possible ABAC policies, and $T = \{t_1, t_2, ..., t_s\}$ is the time intervals for dynamically adjusting MTD configuration. $E = \{E_1, E_2, ....E_n\}$ is the execution tokens allocated to processes, and $I = \{i_1, i_2,....i_x\}$ is the available dynamic network IP addresses.
The objective is to minimize the probability of successful attacks by continuously modifying access control configurations, execution privileges, and network address mappings using an MTD strategy at varying time intervals:

$$\min (R (U, F, P, E, I)) \quad (1)$$

Where R is a function that represents the probability of a ransomware attack succeeding depending on the user file access patterns and access control configurations, which can be modelled as:

$$R(U,F,P,E,I) = \sum_{i=1}^{N} \sum_{j=1}^{M} P(A) \quad (2)$$

Where A is the attack on $f_j$ by $u_i$ through $p_j$, $E_i$, and $I_k$.
The constraints are:
C1: $E_i$ should be assigned based on user privileges
C2: New IP should not conflict with current active sessions
*C3:* Access control policy constraints: $\forall u_i \in U$; $\forall f_j \in F$; $p_j \in P$. This approach ensures that the policies for access control must not conflict with legitimate user activities.
C4: MTD adjustment constraints*:* $\forall u_i, f_j, t_k \in T$. This constraint ensures that adjustments in access control configurations, execution privileges, and network address mappings must occur at predefined intervals without disturbing user activities.
Figure 1 illustrates the overall block diagram of a multilayer defense system using MTD.

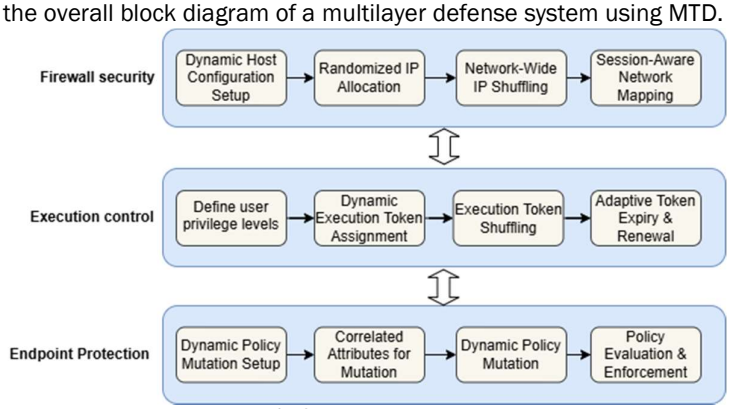


Figure 1. Overall Block Diagram

### 4.3 Firewall Security Using MTD-Based Adaptive Network Address Rotation

In the firewall security layer, MTD is incorporated into Adaptive Network Address Rotation (ANAR) by dynamically shuffling network addresses. This process prevents adversaries from establishing connections and disrupts adversaries trying to evade firewall rules. ANAR is leveraged within a Dynamic Host Configuration Protocol (DHCP) server for periodically reassigning IP addresses to hosts. The firewall ensures that ransomware cannot reliably locate and infect multiple systems by continuously altering network identifiers, significantly minimizing the attack surface. Figure 2 shows the process of MTD-based firewall security using ANAR, where, when an attacker hacks an IP address, they may still fail to compromise the system due to the new IP address.

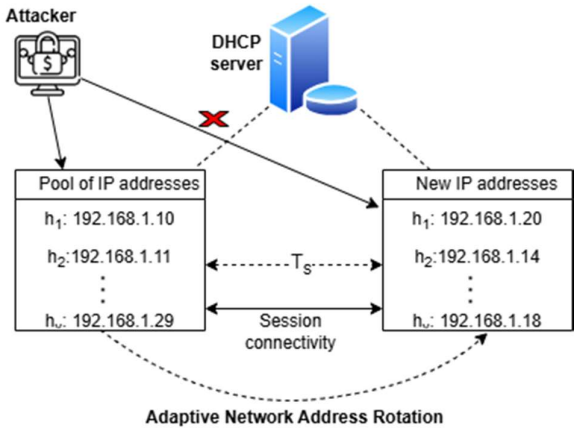


Figure 2. MTD-Based Firewall Security

DHCP server maintains a pool of available IP addresses, which is denoted as I = {$i_1$, $i_2$,..., $i_x$}. An initial randomized IP from I is assigned to network hosts H = {$h_1$, $h_2$, ..., $h_y$} where y ≤ x, ensuring sufficient unique IPs for each system. The shuffling interval ($T_s$) is set dynamically ($T_s \in [T_{min}, T_{max}]$). At every $T_s$, the firewall triggers ANAR in the DHCP server. Each system $h_k$ receives a new IP. The firewall updates its rules dynamically to ensure security. As the critical system connections require session continuity, the firewall tracks active sessions with the help of a session table that logs source and destination IPs, protocol, port numbers, and session status. If the session is not completed after ANAR, the firewall automatically maps the new IP address to the old session to maintain connectivity.

### 4.4 Privilege-Aware Execution Control Using MTD

Conventional privilege-based security models allocate fixed execution permissions to users, making it possible for ransomware to exploit predictable privilege structures for escalating privileges and executing malicious payloads. Hence, MTD is incorporated to improve protection against ransomware by dynamically shuffling execution policies. Hence, it is difficult for the attackers to predict which applications or processes are allowed to execute at any given time, reducing the probability of attacks. Figure 3 shows the process of privilege-aware execution control using MTD.

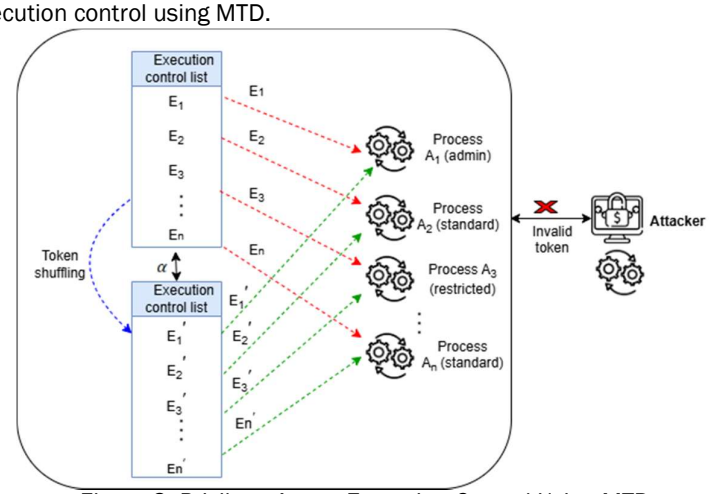


Figure 3. Privilege-Aware Execution Control Using MTD

Every process $A_i$ that requests execution is allocated an execution token $E_i$ based on user privilege levels $L_i$, which is given by $E_i$ = fn ($A_i$, $L_i$), where fn is the token assignment function based on privilege constraints. User privilege levels include admin users who are allowed to run high-risk applications (high-privilege token), standard users who can run only pre-approved applications (moderate-privilege token), and restricted users

who are allowed to access only essential system processes (low-privilege token). Tokens are stored in an execution control list and mapped to process execution policies. Rather than utilizing fixed execution policies, execution tokens are dynamically shuffled after a predefined time interval t. The shuffling event is defined as a Poisson process:

$$\Pr(S_t) = 1 - e^{-\alpha t} \quad (3)$$

Where $\alpha$ indicates the mean shuffling rate and $S_t$ indicates the shuffling event at time t. Shuffling involves reallocating new execution tokens $E_i'$ to processes and modifying which processes are allowed to execute depending on shuffled token validity. The new token is given by $E_i'$ = fn ($E_i$, K), where K is a uniform random variable. The expected time before a token expires follows an exponential decay: D[E] = $1/\alpha$. Before executing the process, the system checks if the allocated execution token is still valid. When an unauthorized process attempts to execute with an invalid token, the system invalidates all current tokens and regenerates new tokens for all the processes with increased token shuffling frequency ($\alpha' = \alpha + \Delta\alpha$) for preventing repeated attempts. $\Delta\alpha$ represents an adaptive increase in shuffling rate depending on attack attempts.

### 4.5 Endpoint Protection Using MTD-Based Access Control

Ransomware exploits static access control rules for escalating privileges and encrypting files. Through the dynamic mutation of access policies at multiple levels, adversaries cannot predict or depend on consistent access paths to encrypt data. By utilizing MTD, access policies are periodically randomized across diverse dimensions such as subject, object, and action, making it difficult for ransomware to escalate privileges and spread. As adversaries can compromise attributes in an ABAC policy, unauthorized access may occur. To address this, hierarchical policy mutation is proposed in which attribute-based rules, sensitivity labels, subject-role mappings, and action constraints are dynamically modified, preventing attackers from predicting and exploiting access control policies. Even when an attacker compromises the subject-object relationship or a particular attribute, access decisions remain unpredictable. Adaptive Hierarchical Policy Mutation (AHPM) is utilized within an ABAC system for improving security against ransomware attacks, as illustrated in Figure 4. Rather than mutating only attribute-based rules, policy evolution is introduced at hierarchical levels to enhance security coverage.

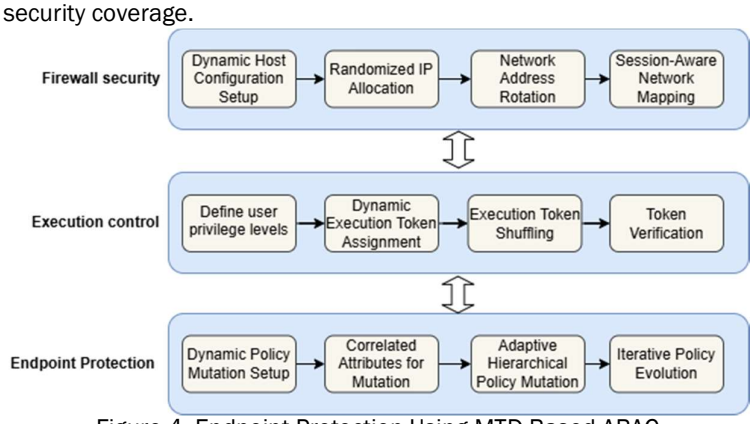


Figure 4. Endpoint Protection Using MTD-Based ABAC

Initially, an ABAC policy P is considered as a set of constraint-based rules R = {$r_1$, $r_2$, $r_3$, ..., $r_k$}, (k > 0). Each $r_i$ governs access decisions depending on attributes related to subjects, objects, and actions. $r_i \in R$ is related to a set of attributes $S_{r_i}$, which captures the relevant features of subjects, objects, and actions. For generating a mutated policy P′, the mutation process is performed by dynamically altering diverse dimensions like subject, object, and action. Subject-level mutation randomly fine-tunes subject-role mappings for interrupting predictable privilege escalation pathways. The user usually allocated with a specific role may have their privileges modified or reallocated based on contextual factors. Object-level mutation dynamically recategorizes objects such as files by altering sensitivity labels. For instance, an asset formerly considered low-risk might be redefined as high-risk based on real-time assessments, thereby preventing adversaries from constantly targeting high-value assets. Action-level mutation randomizes permitted actions on objects based on varying behavioural patterns. The actions a user is permitted to execute—such as read, write, or delete—can dynamically alter based on observed behavioural patterns.

For each rule $r_i \in R$, the set of correlated attributes $Z_c$ is identified, where $Z_c \approx S_{r_i}$. $r_i$ is transformed into a new rule $r_i'$ by randomly selecting an attribute $z \in Z_c$ and incorporating it into $S_{r_i}'$, where $S_{r_i}' = S_{r_i} \cup z$. The system analyses $S_{r_i}$ and examines attribute-to-access relationships that lead to granted permissions, creating a baseline for valid access control conditions. The system scans $Z_c$ to find new attributes ($Z_c'$) that are strongly correlated with those in $S_{r_i}$. These correlations are derived from past access patterns, behavioural analysis, and real-time interactions among objects, subjects, and actions. $Z_c'$ acts as the potential candidates for policy mutation. The system assesses whether adding $Z_c'$ to $S_{r_i}$ would affect

legitimate access and introduce unauthorized access. In order to balance security and usability, adjustments are made. A new set of modified rules $R' = \{r_1', r_2', \ldots, r_n'\}$ is formed to define the mutated policy $P'$. For enforcement, $P'$ is forwarded to a policy evaluation module. For introducing variability across all policy levels, the mutation process is periodically repeated, ensuring that attackers cannot depend on static access rules.

**Algorithm: Multilayer Ransomware Defense Using MTD**

////Firewall Security////

Initialize a pool of available IP addresses $I = \{i_1, i_2, \ldots i_x\}$ in DHCP server

Assign I to network hosts $H = \{h_1, h_2, \ldots, h_y\}$ where $y \leq x$

Set $T_s \in [T_{min}, T_{max}]$

for each $T_s$ do

    Perform network-wide IP shuffling.

    $h_k$ receives a new IP

endfor

Updates IP addresses dynamically

Automatically maps the new IP address to the old session //session connectivity//

//Execution Control//

Determine user privilege levels $L_i$ for processes $A_i$

Calculate execution token $E_i = fn(A_i, L_i)$

Assign $A_i$ with $E_i$ based on $L_i$

Store $E_i$ in an execution control list and map to process execution policies.

Determine shuffling probability

Calculate new execution tokens $E_i' = fn(E_i, K)$

Reallocate $E_i'$ to $A_i$

If the allocated execution token is still valid then

    Execute the process

else

    Invalidates all tokens and regenerates new tokens for all $A_i$

    Increase token shuffling frequency ($\alpha' = \alpha + \Delta\alpha$)

End if

//Endpoint Protection//

Initialize ABAC policy with rules $R = \{r_1, r_2, r_3, \ldots, r_k\}$

$r_i \in R$ is related to $S_{r_i}$

For each $r_i \in R$,

    Identify $Z_c$, where $Z_c \approx S_{r_i}$

    Perform subject-level, object-level, and action-level mutation.

    Scans $Z_c$ to find $Z_c'$ that are strongly correlated with those in $S_{r_i}$

    If adding $Z_c'$ to $S_{r_i}$ would affect legitimate access and introduce unauthorized access then

        New attributes are selected and perform step 33

    Else

        $r_i \rightarrow r_i'$ by randomly selecting $z \in Z_c$ and incorporating it into $S_{r_i}'$

        Generate P′

    endif

endfor

Repeat periodically

end

## 5. Results and Discussion

### 5.1 Experimental Setup

This section presents the experimental setup utilized to assess the proposed multilayer defense strategy using MTD. The experiment includes various parameters, configurations, and security metrics for assessing the efficiency of the defense mechanisms under realistic threat conditions. The key security metrics, such as PoC, AR, IRV, ESTV, and PMV– were considered for individual hosts and systems based on their service vulnerabilities, exposure levels, and criticality within the network topology. The MTD strategies were verified in a controlled environment simulating real-world ransomware attack scenarios. The setup included 100 interconnected hosts, each running two distinct services, with different IP addresses. 100 processes were simulated across all virtual machines (VMs), averaging 20 for each VM, including 10 critical system processes (such as `sshd`, `systemd`, `svchost.exe`), five user-level services, and 5 simulated ransomware-related attacker processes such as encryption routine (ER), privilege escalation script (PES), command-and-control (C2) beacon, lateral movement (LR) tools, and file enumeration scanner (FES). Adaptive MTD approaches – including rotation, shuffling, and mutation – were periodically triggered to modify the system's configuration dynamically. These approaches were implemented in response to predefined intervals and simulated threat activity, while balancing security enhancement with operational cost. Attack simulations followed a structured adversary behaviours modelled on frameworks, specifically replicating ransomware attack patterns across both broad and targeted attack scenarios.

Attackers that successfully exploit system components can simulate command and control behaviours. However, MTD mechanisms such as firewall, execution control, and ABAC-based endpoint security disrupted ongoing ransomware activities by dynamically changing access permissions, terminating malicious processes, and implementing context-aware restrictions, thus forcing attackers to restart reconnaissance. These defenses interrupted attacker growth, increasing the cost and minimizing the probability of success. The metrics gathered after each adaptive change confirmed a consistent reduction in attack success, an increase in variability, and overall improved system resilience, validating the efficiency of the proposed approach.

The performance metrics considered are:

- **IP Rotation Variability (IRV):** It evaluates the degree of unpredictability introduced in network communication by recurrently rotating IP addresses to prevent reconnaissance and scanning attacks.

- **Execution Token Shuffling Variability (ETSV):** It measures the randomness in execution control flows by dynamically shuffling execution tokens, thereby reducing the probabilities of attacker success in process hijacking.
- **Policy Mutation Variability (PMV):** It captures the variability in dynamically modifying access control policies to limit predictability and alleviate privilege escalation attacks.
- **Probability of Compromise (PoC)** measures how probably a ransomware attack is to successfully compromise a system, depending on vulnerabilities, exposure levels, and attacker capabilities.
- **Attack Risk (AR)** provides an overall assessment of the network's exposure to ransomware attack while considering VM vulnerabilities, service weaknesses, and connectivity.

References


1. Nayak, S. C., Tiwari, V., & Samanthula, B. K. (2023, March). *Review of ransomware attacks and a data recovery framework using Autopsy digital forensics platform*. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0605–0611). IEEE. https://doi.org/10.1109/CCWC57344.2023.10099169
2. Kritika, E. (2024, November). A comprehensive literature review on ransomware detection using deep learning. *Cyber Security and Applications*, *100078*. https://doi.org/10.1016/j.csa.2024.100078
3. Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., & Bilan, O. (2021, September). *Ransomware attacks: Risks, protection and prevention measures*. In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 473–478). IEEE. https://doi.org/10.1109/ACIT52158.2021.9548507
4. Vasoya, S., Bhavsar, K., & Patel, N. (2022, January). A systematic literature review on ransomware attacks. *arXiv*. https://doi.org/10.48550/arXiv.2212.04063
5. Sharma, P., Kapoor, S., & Sharma, R. (2022). Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach. *International Journal of Systems Assurance Engineering and Management*, *14*(1), 287–296. https://doi.org/10.1007/s13198-022-01793-0
6. Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business & Cyber Security (IJBCS)*, *1*(2), 52–60. Academy of Business and Retail Management (ABRM).
7. Zhang, T., Li, Y., Wang, M., Chen, H., Zhao, J., & Liu, Y. (2025). Moving target defense meets artificial intelligence-driven network: A comprehensive survey. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2025.3533016
8. Brown, A., Lee, T.-W., & Hong, J. B. (2023, May). Evaluating moving target defenses against realistic attack scenarios. In *2023 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)* (pp. 1–8). IEEE. https://doi.org/10.1109/EnCyCriS59249.2023.00005
9. Mercado-Velazquez, A. A., Escamilla-Ambrosio, P. J., & Ortiz-Rodriguez, F. (2021). A moving target defense strategy for Internet of Things cybersecurity. *IEEE Access, 9*, 118406–118418. https://doi.org/10.1109/ACCESS.2021.3107403
10. Sun, R., Zhu, Y., Fei, J., & Chen, X. (2023). A survey on moving target defense: Intelligently affordable, optimized and self-adaptive. *Applied Sciences, 13*(9), 5367. https://doi.org/10.3390/app13095367
11. Viking Cloud. (2025). *170 cybersecurity stats and facts for 2025*. https://www.vikingcloud.com/blog/cybersecurity-statistics#16
12. Pagan, A., & Elleithy, K. (2021). A Multi-Layered Defense approach to safeguard against ransomware. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 0942–0947. https://doi.org/10.1109/ccwc51732.2021.9375988
13. Xu, K., Li, Z., Liang, N., Kong, F., Lei, S., Wang, S., Paul, A., & Wu, Z. (2024). Research on Multilayer Defense against DDoS Attacks in Intelligent Distribution Networks. *Electronics*, *13*(18), 3583. https://doi.org/10.3390/electronics13183583
14. Ryu, D., Lee, S., Yang, S., Jeong, J., Lee, Y., & Shin, D. (2024). Enhancing cybersecurity in energy IT infrastructure through a layered defense approach to major malware threats. *Applied Sciences*, *14*(22), 10342. https://doi.org/10.3390/app142210342
15. Denis, J., Featherstone, J., Beaufort, O., & Edelstein, H. (2024). A Novel Algorithmic Framework for Autonomous Ransomware Detection Using Multilayer Temporal Anomaly Patterns. *OSF Preprints*. https://doi.org/10.31219/osf.io/g7yku
16. Mofidi, F., Hounsinou, S. G., & Bloom, G. (2024). L-IDS: A Multi-Layered Approach to Ransomware Detection in IoT. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 0387–0396. https://doi.org/10.1109/ccwc60891.2024.10427870

17. Qiu, Y., Wu, J., Mumtaz, S., Li, J., Al-Dulaimi, A., & Rodrigues, J. J. P. C. (2021). MT-MTD: Muti-Training based Moving Target Defense Trojaning Attack in Edged-AI network. *ICC 2022 - IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/icc42927.2021.9500545
18. Rehman, Z., Gondal, I., Ge, M., Dong, H., Gregory, M., & Tari, Z. (2024). Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. *Computers & Security*, *139*, 103685. https://doi.org/10.1016/j.cose.2023.103685
19. Gayathri, R., Usharani, S., Mahdal, M., Vezhavendhan, R., Vincent, R., Rajesh, M., & Elangovan, M. (2023). Detection and mitigation of IoT-Based attacks using SNMP and moving target defense techniques. *Sensors*, *23*(3), 1708. https://doi.org/10.3390/s23031708
20. Masud, M. T., Keshk, M., Moustafa, N., Turnbull, B., & Susilo, W. (2025). Vulnerability defence using hybrid moving target defence in Internet of Things systems. *Computers & Security*, 104380. https://doi.org/10.1016/j.cose.2025.104380
21. Huang, C., Liu, I., Li, J., Wu, C., Li, C., & Liu, C. (2021). A Legacy Infrastructure-based Mechanism for Moving Target Defense. *2021 IEEE 3rd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, 80–83. https://doi.org/10.1109/ecbios51820.2021.9510261
22. Von Der Assen, J., Celdrán, A. H., Sánchez, P. M. S., Cedeño, J., Bovet, G., Pérez, G. M., & Stiller, B. (2023). A lightweight moving target defense framework for multi-purpose malware affecting IoT devices. *ICC 2022 - IEEE International Conference on Communications*, 6010–6015. https://doi.org/10.1109/icc45041.2023.10278951
23. Von Der Assen, J., Celdrán, A. H., Sefa, R., Stiller, B., & Bovet, G. (2024). MTFS: a Moving Target Defense-Enabled File System for Malware Mitigation. *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, 1–6. https://doi.org/10.1109/lcn60385.2024.10639803
24. Liu, S., & Chen, X. (2023). Applying Moving Target Defense Against Data Theft Ransomware on Windows OS. *MDPI*. https://doi.org/10.20944/preprints202312.0948.v1
25. Khan, M. M., Hyder, M. F., Khan, S. M., Arshad, J., & Khan, M. M. (2022). Ransomware prevention using moving target defense based approach. *Concurrency and Computation Practice and Experience*, *35*(7). https://doi.org/10.1002/cpe.7592
26. Celdrán, A. H., Sánchez, P. M. S., Von Der Assen, J., Schenk, T., Bovet, G., Pérez, G. M., & Stiller, B. (2024). RL and Fingerprinting to Select Moving Target Defense Mechanisms for Zero-Day Attacks in IoT. *IEEE Transactions on Information Forensics and Security*, *19*, 5520–5529. https://doi.org/10.1109/tifs.2024.3402055
27. Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2023). Ransomware early detection: A survey. *Computer Networks*, *239*, 110138. https://doi.org/10.1016/j.comnet.2023.110138
28. Lei, C., Zhang, H., Tan, J., Zhang, Y., & Liu, X. (2018). Moving Target Defense Techniques: a survey. *Security and Communication Networks*, *2018*, 1–25. https://doi.org/10.1155/2018/3759626