VER
Vascular & Endovascular Review

An Optimized Model for Plan and Tent Security Services and Identification of attacks

Binu C T[1], Rubini.P[2]

[1]Scholar, SOET, CMR University, Email: binuct143@gmail.com
[2]professor, SOET, CMR University, Email: Rubini.p@cmr.edu.in

ABSTRACT

Security in a multi-cloud environment involves securing data, applications, and infrastructure across multiple cloud providers (e.g., AWS, Azure, Google Cloud). A strong security model is essential to reduce risk, maintain compliance, and ensure visibility and control. The proposed security model that provide an optimized security based on security sensitivity and trust level. High level security is offered when the security sensitivity(ss) value between -1 and 1.Trust level(TL) value is based on trust Model that evaluates TL value between 0 and 1.There is a function to evaluate security sensitivity and trust level. Initial value of SS is 0.75 and TL is 0.83.Key management is done rapidly and securely.IPspec Collector helps to find all the type of attacks to Cloud environment.

KEYWORDS: Plan and Tent Security,Trust Model,Security Sensitivity,Trust Level,Key management,identification of attacks

How to Cite: Binu C T, Rubini.P, (2025) An Optimized Model for Plan and Tent Security Services and Identification of attacks, Vascular and Endovascular Review, Vol.8, No.1s, 215-219.

INTRODUCTION

Zero Trust Security Model have a principle "Never trust, always verify and its application include Every request is authenticated and authorized, regardless of origin.Micro-segmentation and least privilege access.Identity-aware proxy and continuous monitoring.Shared Responsibility Model Principle include Security is a shared responsibility between the cloud provider and the customer and its applications areProviders secure the infrastructure (hardware, networking, etc.).Customers secure their data, user access, and workloads. Varies slightly by provider (AWS vs. Azure vs. GCP).Identity and Access Management (IAM) have focus on Unified identity across clouds using federated identity management and its best practice include Use centralized IAM solutions (e.g., Azure AD, Okta, AWS IAM Federation).Implement role-based access control (RBAC).Enable Multi-Factor Authentication (MFA).Cloud Security Posture Management (CSPM) focus on Continuously assess and manage cloud security risks and its capabilities are Detect misconfigurations,Enforce compliance (e.g., HIPAA, GDPR, ISO 27001) and Provide automated remediation.Data Protection Model is focusing on Protect data in transit, at rest, and in use.

- **Best Practices**:
  - End-to-end encryption (TLS, AES-256).
  - Use Key Management Services (KMS) across cloud platforms.
  - Tokenization and data masking.

Unified Threat Detection & Response focus on Centralize threat detection across cloud environments.

- **Tools**:
  - SIEM/SOAR platforms (e.g., Splunk, Microsoft Sentinel).
  - Cloud-native tools (AWS GuardDuty, GCP Security Command Center).
  - Endpoint Detection & Response (EDR).

Compliance and Governance Framework focus on how Ensure adherence to legal and regulatory standardsand the Strategies are
  - Implement multi-cloud governance policies.
  - Automate audits and reporting.
  - Use frameworks like NIST, CIS Benchmarks, or ISO.

Secure DevOps (DevSecOps) focusing on operation to Integrate security into CI/CD pipelines and the tactics are Shift-left testing for vulnerabilities,Use Infrastructure as Code (IaC) scanning (e.g., Terraform scans) and Automate security checks in builds.

Tools & Technologies for Multi-Cloud Security

Function	Tools
IAM & SSO	Okta, Azure AD, Auth0
CSPM	Prisma Cloud, Wiz, Lacework
SIEM	Splunk, IBM QRadar, Azure Sentinel
Encryption & KMS	AWS KMS, Azure Key Vault, Google KMS

Function	Tools
DevSecOps	Snyk, Checkov, Aqua Security

LITERATURE SURVEY

1. Cyber Security Monitoring in the Maritime Domain
- Risto Vaarandi et al., arXiv (March/April 2025)
- Focuses on maritime-sector cybersecurity monitoring—specifically automated detection methods for detecting threats in IT/OT systems.
- Provides bibliometrics, taxonomy of techniques, and identifies key gaps and future direction

2. Cyber Attacks & Security Challenges: Threats, Countermeasures, and Future Directions
- Taha Riaz, University of Management & Technology (Feb 2025)
- A systematic literature review that synthesizes recent findings on topical cyber-threats, countermeasures, and future avenues.

3. Large Language Models for Cybersecurity: A Survey
- Hanxiang Xu et al., May 2024
- Reviews applications of LLMs (e.g. GPT style models) for malware analysis, intrusion detection, phishing detection, etc., drawing insights from 127 high quality papers. Highlights dataset limitations and need for greater interpretability.

4. Security & Privacy Challenges of Large Language Models
- Badhan Chandra Das et al., Jan 2024
- Examines vulnerabilities in LLMs such as data poisoning, PII leakage, jailbreaking, and discusses defense mechanisms and research gaps.

5. Collaborative Cybersecurity Using Blockchain
- Loïc Miller & Marc Oliver Pahl, Mar 2024
- Reviews blockchain-based decentralized approaches for threat intelligence sharing, access control, and trust management. Offers guidelines and identifies fragmentation in consensus protocol selection.

6. IoT Security Review
- MDPI (2023 early 2024)
- Discusses categories such as identity management, attack detection, data protection, risk management, with a special emphasis on ML, blockchain, edge/fog computing solutions. Highlights challenges like resource constraints and concept drift.

7 Security Maturity Assessment
- Fresh SLR (Aug 2024)
- Covers organizational maturity models in cyber/information security—implementation status, industry adoption, drivers and challenges—based on PRISMA guidelines. Final set includes 96 studies.

8. Cyber Security Datasets & Semi Supervised Models
- Discover Data, April 2023
- Reviews publicly available cybersecurity datasets and metrics used in semi supervised learning, covering domains like intrusion detection, malware, phishing, botnet detection.
- Internet Measurement Techniques in Cybersecurity
- ScienceDirect review (2023)
- Presents taxonomy of measurement approaches for cyber threats, analyzing methodology, scope, and future directions.

Emerging Concepts Across Surveys
- Large Language Models & AI-based Security: Rapidly evolving with both potent use cases (LLM based detection, threat analysis, proactive hunting) and serious vulnerabilities (privacy breaches, adversarial manipulation, lack of interpretability)
- Blockchain & Collaborative Intelligence: Investigated as a trust-enhancing tool for secure sharing and decentralized control—but still fragmented and immature in standardization.
- IoT & Edge based Defenses: Strong focus on identity management, anomaly detection, data protection, blockchain, edge/fog computing—but constrained by limited device resources and rapid threat changes
- Cybersecurity Maturity & Policy Models: Evaluating how organizations adopt and implement maturity models, with an emphasis on risk, governance, compliance frameworks

Context & Trends in the Broader Cybersecurity Landscape

Recent surveys and industry reports reveal:
- Widespread policy bypass: Engineers frequently circumvent security controls; true zero trust is yet limited in implementation. nypost.comitpro.com

- Rising complacency: Despite risks, companies often underprepare for cybercrime amplified by AI technologies. Compliance regimes (e.g. EU NIS2, DORA, upcoming UK bill) are emerging globally. Reuters+1ft.com+1
- Skills gap critical issue: Organizations face growing difficulty staffing skilled cybersecurity professionals—upskilling is being promoted. itpro.com
- Tool sprawl & insufficient visibility: Security teams sacrifice visibility, quality, coherence under operational pressure, undermining effectiveness in complex environments with AI-augmented threats

PROPOSED SYSTEM

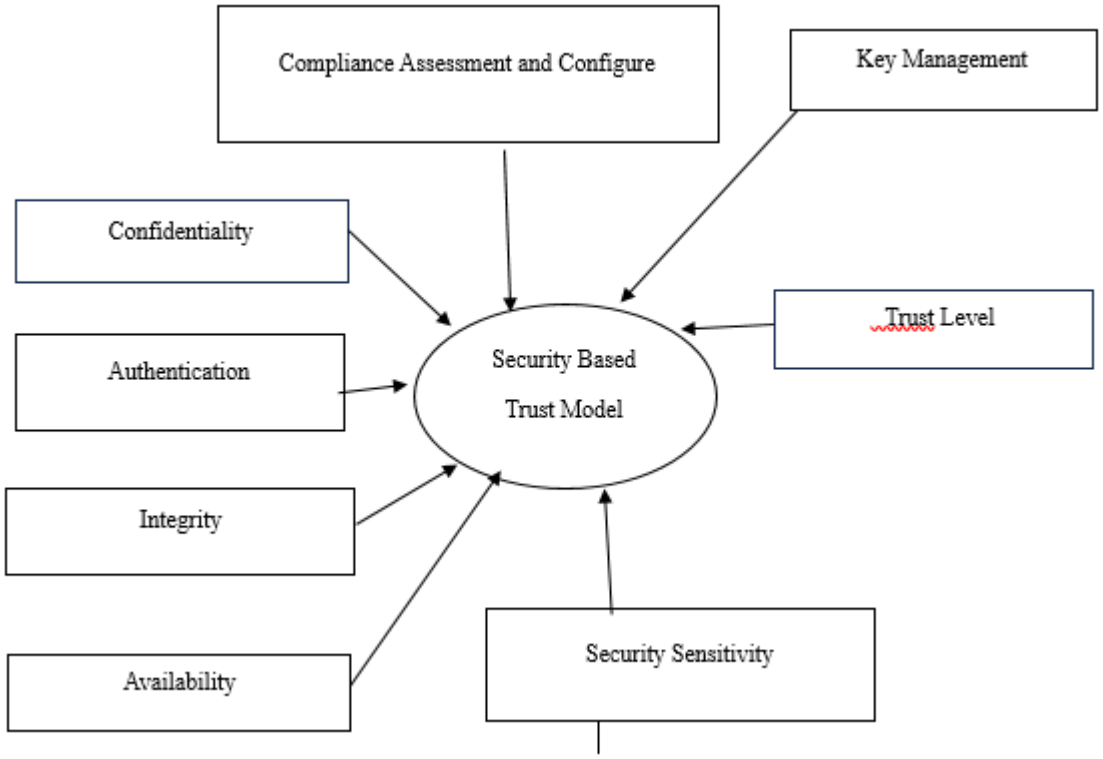

Fig1: Security based Trust model

Confidentiality is doing with encryption and decryption based on digit sum. Authentication is done based on crypto password. Integrity is calculated by Cij=Cij+Ci||Cj.Availability is calculated by e^x-1 .Security Sensitivity is based on differential equation n with two function f(x) and g(x).Trust Level is calculated by using the function f(y) and g(y).Complaince Assessemnt and Configure based on trust model.The repetitive value of Secuirty Sensitivity and Trust Level shows the Optimized Security by Plan and Tent Security Services Existing Algorithms evaluates security sensitivity by cos(theta) and trust level by tan(theta).where theta is the speed. Security Sensitivity and Trust Level is measured and find the solution.

Initial value of x=0.75
f(x)=cos(theta)-x+1
g(x)=|tan(theta)-f(x)+1|
Security Sensitivity SS=df(x)/dx-|g(x)|
Initial value of y=0.83
f(y)=tan(theta)-y+1
g(y)=|cos(theta)-f(y)+1|
Trust Level TL=f(y)+|g(y)|

Key management is done based on SS and TL values.The matrics of key are used to encrypt and decrypt.{k1,0,0},{0,k2,0}{0,0,k3} is used when TL value is 0 and SS value is between 0 and -1,The key value {k1,0,0},{k2,k3,0}{k4,k5,k6} is used for the other cases.

IDENTIFICATION OF ATTACKS

Different types of attacks are identified using IPSpec Collector object.Each one is identified by a key.

```
void ip()
{
while(1)
{
```

```
switch(IPSpec Collector)
{
 case "make":
 printf("sql injection")
 break;
 case "sense":
 printf("evedropping")
 break;
 case "pole":
 printf("API Hacking")
 break;
 case "ready":
 printf("phishing")
 break;
 break;
 case "para":
 printf("cloud service abuse")
 break;
 case "can"
 printf("Deniel of service")
 case "do":
 printf("Malicious Attack")
 break;
 case "common":
 printf("cloning")
 break;
 case "virtual"
 printf("XML Signature Attack")
 break;
 case "collect"
 printf("Flooding Attack")
 break;
}
}
}
```

DATA ANALYSIS

Cos(180) have the value -1 and find out the value is SS (Security Sensitivity) by find and applying the values if f(x) and g(x).The repeated values and entries shows that there is optimized security to multi cloud for real time application. Similarly for Trust Level .Result is obtained from the dataset(y) and g(y) are used to get TL

Security	Security Sensitivity
-1	0.75
-1	-3.5
-1	-1
-1	-1

Table 1: SS and security

Security	Trust Level;
-1	0.83
-1	0

-1	2
-1	0
-1	0

Table 2: TL and security

RESULT AND DISCUSSION

An Optimized security is provided by the security services when there is a repeated entries of TL and SS value.There is a straight line graph for existing system and the optimized security shows that values are reparted after some time.Security Sesitivity is reduced after data transfer starts and TL values increase at the same time.SS value -1 indicates that there is an optimized security and TL value 0 indicates the same.

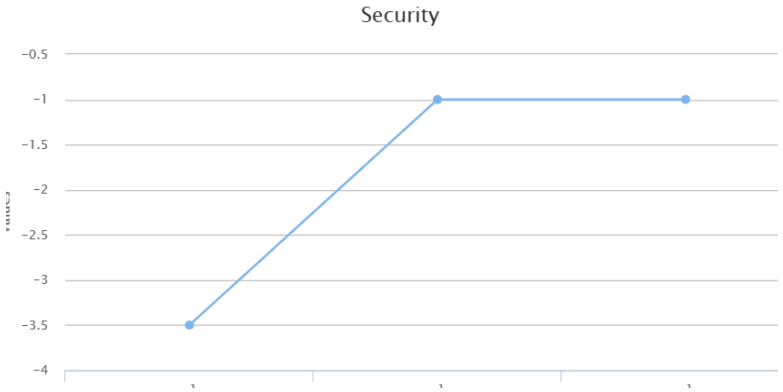

Fig 2: Security Sensitivity graph

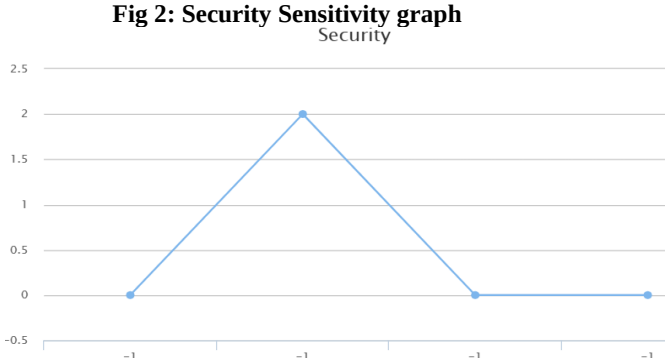

Fig 3: Trust level graph

REFERENCES

1. Bin Liu “A Survey on Trust Modeling from a Bayesian Perspective” (2018) Springer Nature Volume 112, pages 1205–1227, (2020).
2. M. Momani and S. Challa, “Survey of Trust Models in Different Network Domain,” International Journal Ad Hoc, Sensor & Ubiquitous Computing, Vol. 1, No. 3, 2010, pp. 1-19. doi:10.5121/ijasuc.2010.1301.
3. Himani Tyagi , Rajendra Kumar , Santosh Kr Pandey A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions panel .
4. Jiang, Tseng, “Trust Model for Wireless Network Security Based on Edge Computing” 2021.
5. Aaqib, M., Ali, A., Chen, L. *et al.* IoT trust and reputation: a survey and taxonomy. *J Cloud Comp* **12**, 42 (2023). https://doi.org/10.1186/s13677-023-00416-8.