Security Landscape of a Strong Ecosystem to Protect Sensitive Information in E-Governance

Dr. Saurabh Gupta[1], Anup Kumar[2], Piyushank Gupta[3]

[1]Scientist G, National Informatics Centre, New Delhi, India
[2]Scientist C, National Informatics Centre, New Delhi, India
[3]Scientist D, National Informatics Centre, Lucknow, Uttar Pradesh, India

---***---

Abstract - *Today, with the ascent of The Digital Personal Data Protection Act, 2023 and strict amendments to IT ACT, there is a need to strike a balance between data privacy and data processing for lawful purpose. Unchecked processing may have adverse implications on the privacy of individuals, as well as can be threat to the state, if data is of secret nature. Protecting citizens' data during its entire life cycle needs a strong ecosystem and adherence to existing global data protection regulations like GDPR and security standards such as PCI- DSS, HIPAA etc. This paper presents a holistic approach to enhance the Cyber Security landscape of government organizations as per the sensitivity of the data during its access, processing and dissemination, thus keeping the data privacy of individuals intact. The approach is to map an organization's data security classification with the appropriate security posture so that the data can be protected using appropriate mechanism as per the classification of data and to enhance its security landscape using Indian government guidelines, advisories and global standards.*

Key Words: Cyber Security, Digital Personal Data Protection Act, Data Security Classification, Defense in Depth, Security by Design

1. INTRODUCTION

With the advancement in Cyber Security technology and methodologies, we have numerous security appliances and software solutions to ponder upon while considering the establishment of robust infrastructure in an organization to protect data. Security Operations Center (SOC) has also been evolved a lot right from presence of antivirus and firewall in SOC v1 to Security Information and Event Management (SIEM) & Security Orchestration Automation and Response (SOAR) in Next Gen SOC. In this evolution process, SOC has got Data Loss Prevention (DLP) in place along with the focus on Bring Your Own Device (BYOD) policies [11] and Zero Trust Architecture (ZTA) [9]. Since these tools and security solutions involves a lot of cost and an organization cannot have each of them in place to protect data, it is highly recommended to classify the data into different categories based on their sensitivity before implementing a Defence in Depth strategy [13]. In fact, the security classification [3] of data should be the first step in path of establishing an Information Security Management System (ISMS) and SOC in an organization. Security classification not only enables an organization to decide the security controls to put in place based on the sensitivity of data but also makes it easy to comply or follow the global Cyber Security Frameworks and Standards. To classify the data, organizations can follow their own classification rules but the overall instructions and guidelines are given in Manual of Departmental Security Instructions issued by Ministry of Home Affairs (MHA). The document is comprehensive and defines the procedures to classify the data into various categories. The organizations' internal data security classification can be mapped to one of the categories defined in this document. In the presented approach, we classify the data into three categories viz Category X, Category Y and Category Z where Category X is considered as highly sensitive, Category Y as sensitive and Category Z as restricted as shown in Table - 1.

Category	Sensitivity	Type of Data
X	Highly Sensitive	Leakage of which causes grave damage to the organization and its functioning
Y	Sensitive	Leakage of which causes either damage to the organization or causes embarrassment
Z	Restricted	Data related to digital personal data leakage of which may cause violation of privacy laws

Table -1: Data Classification

Above classification is just for reference and is used in the scope of the paper. An example is presented here [4]. After the data classification is complete, the approach is to discuss the Cyber Security landscape of the Information and Communication Technology (ICT) infrastructure handling the data that is mapped under these three categories.

It is to be noted that the data which is of Secret or Top Secret nature and is of national importance, is outside the scope of approach discussed. In this approach, a holistic view of security posture is given to reduce the attack surface at each layer thereby enhancing the overall security landscape shown in Fig. 1. The layered approach of the defense mechanism for these three categories is discussed in further sections.

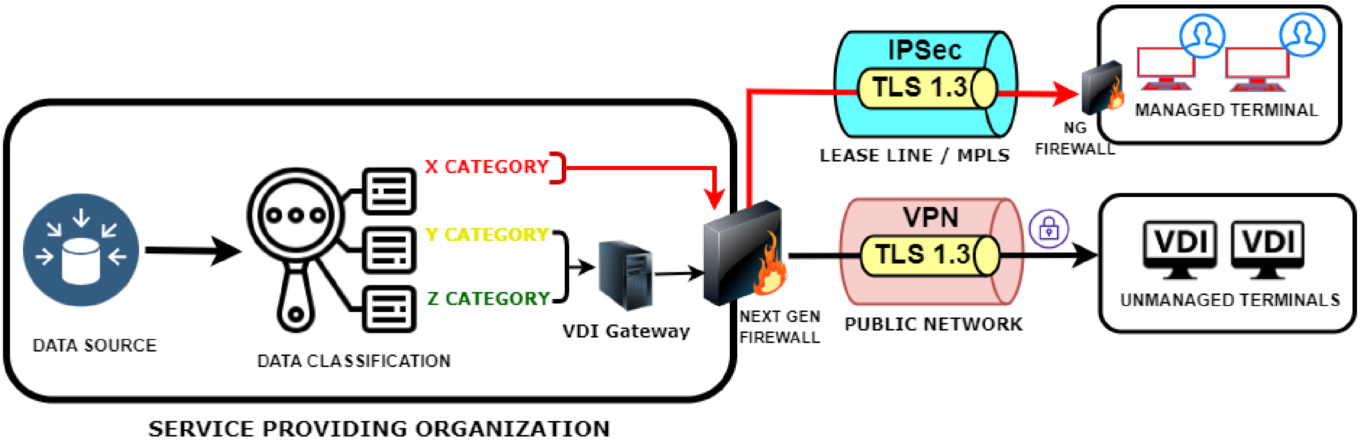

Fig -1: Access Mechanism as per Data Category

2. PHYSICAL LAYER SECURITY

Physical Layer forms the foundation of all higher layers in an OSI model and is required first to be protected to keep data at higher layers safe. It includes restricting physical access with the help of physical security policy that clearly defines the guidelines considering the three categories of data. Category X data is made available to the users only on managed endpoints/terminals which are placed in closed environment with proper physical access controls. These managed terminals are placed at user's premise but are managed remotely by the organization which is storing and processing this data. These managed terminals are properly hardened and do not available on public networks or Internet. The admin privileges of these terminals are revoked so that these are fully in control of the organization managing them. Category Y and Category Z data can be accessed over unmanaged terminals governed by BYOD policies which are covered in further sections.

3. DATA LANK LAYER SECURITY

Data Link layer is the second layer of the OSI model that is primary responsible for framing data packets and their transmission over physical network. This layer does not handle data encryption directly but provides different mechanisms to ensure integrity and authenticity of data. The use of managed switches is recommended so that security options at Data Link layer can be applied. The security landscape at Data Link layer consists of following:

3.1 MAC Address Filtering

Managed switches provide the option of port security where each and every port is having the MAC (Media Access Control) address of the device connected to it. Any change in device connected to that port is straightly denied by the switch. This prevents connecting unauthorized devices to connect to the organization's network. All managed terminals, firewalls must be connected to managed switches with proper MAC bindings.

3.2 Virtual Local Area Networks (VLAN)

Managed switch enables the creation of VLANs, the Virtual Private Network which logically segments LAN (Ethernet) into virtual LANs. Each LAN is having its own VLAN ID. This enhances the security by preventing data from one VLAN to cross into other VLAN. This also reduces broadcast traffic from switches.

3.3 ARP Spoofing Protection

ARP spoofing (Address Resolution Protocol spoofing) is a type of cyber-attack where an attacker sends malicious ARP messages to a local network. The goal of ARP spoofing is to associate the attacker's MAC address with the IP address of another legitimate device on the network, diverting network traffic intended for that legitimate device to the attacker's system. Managed switches enable the protection from spoofed or fake ARP packets to prevent man in the middle attack at the Data Link layer. Additionally, static ARP table entries are recommended to prevent ARP spoofing.

3.4 Security Patches

Managed switches allow the patching of security fixes of firmware as and when they are available. Automated patching of all networking devices using centralized patch management is done. Centralized patch management uses a central server that checks network hardware for missing patches, downloads the missing patches and distributes them to the managed terminals and other networking devices on the network in accordance with the organization's patch management policy. For Category X data that do not connect to Internet, the patch management is done in offline mode on regular basis.

4. NETWORK LAYER SECURITY

The network layer is third layer of OSI model which consists of actual data in the form of data packets. It consists of router, firewall as primary devices. Securing this layer is essential to protect data, maintain network availability, prevent unauthorized access, and comply with regulatory requirement.

Following security posture should be considered as per the category of data:

4.1 Establishment of Demilitarized Zone (DMZ)

Demilitarized Zone is used to place devices that use Internet or any public network for external communication. These devices may include Network Time Protocol (NTP) servers, Email Servers, Domain Name Server (DNS) etc. in case these servers communicate to external network. For Category X data, dedicated internal NTP Server, Email Server and DNS Server are to be used. For Category Y and Category Z data, all components doing external communication are to be placed in DMZ zone of organizations network.

4.2 Firewall and IPSec

The Next Gen firewall is state of the art equipment for modern SOC which can operate at each layer of Open System Interconnect (OSI) model. For Category X and Y data, firewalls should have Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) enabled. In addition to traffic inspection, these firewalls can host IPSec VPN to provide encryption for data in transit. For Category X data which are available only on managed terminals that are behind managed firewall, Internet Protocol Security (IPSec) is to be applied between firewalls. An IPSec is a network layer VPN that provides network layer encryption. In all categories, traffic inspection using North-South firewall is essential. Regular processing of Cyber Threat Intelligence received from Original Equipment Manufacturers (OEMs) and Organizations such as CERT-In are to be implemented to protect each category of data.

4.3 NAT and ACL

Network Address Translation (NAT) should be enabled at the network gateway (router, firewall etc.) to hide internal private IP addresses. ACL (Access Control List) are applied at router which are rules that define which network traffic is allowed and which is denied. All categories of data are required to have ACLs applied at routers. Category X data are required to have NAT enabled at routers.

4.4 Use of East-West Firewalls

Network has to be segmented into security zones making use of East West Firewalls to monitor lateral traffic for thwarting any security breach. It also limits the impact of security breach within the compromised network segment. Firewalls should be used to monitor east-west traffic in addition to north-south traffic. These firewalls logically segment the network into various security zones by setting up policies over traffic between components inside data centre (DC) such as server to server traffic, traffic between micro services, traffic between one networking devices to other, traffic between virtual machines etc. Servers should not communicate to each other unless they are part of same application with dedicated ports. Infrastructure handling Category X data should be segmented from infrastructure handling Category Y and Z data using East West firewall.

4.5 Use of Dedicated Connectivity

Category X data is available on logically separated connections only that include MPLS, leased lines. Managed terminals that handle Category X data only, are connected using this separated or dedicated connectivity. VPN is used to add encryption layer as these networks do not provide any encryption, by default.

Category Y & Z data can be made available over public networks but using encrypted channel over Virtual Desktop Infrastructure and additional security features provided by other layers

4.6 Network Access Control

Network Access Control (NAC) is used to manage and regulate access of network devices in a Data Centre (DC) environment. It ensures that only authorized and compliant device can connect to a network. A NAC also helps in implementing the BYOD policy and guest user management within an organization or DC by doing end point security posture check for its compliance.

Organization's processing Category X & Y data are recommended to have implemented NAC to manage their IT infrastructure.

5. TRANSPORT LAYER SECURITY

Transport layer is the fourth layer of OSI model that is responsible for end to end transportation of packets. Transport Layer is typically handled by the Operating System/Firmware of various Endpoints and networking devices due to which anything that is used to manage endpoints are kept under this layer. Security of Transport Layer consists of following:

5.1 Unified Endpoint Management

Unified Endpoint Management (UEM) tools are used to manage endpoints of a network. UEM not only monitors the endpoints but also does patch management. Security patches to Operating System, software applications, application of policies at OS level are automated with help of UEM.

Endpoints include workstations of SOC (Security Operations Centre), NOC (Network Operations Centre), Servers, etc. inside data center as well as Managed Terminals. Since security management of endpoints are most important for enhancing security landscape of an organization, use of UEM is highly required for managing terminals handling all categories of data.

5.2 Use of DLP, EDR and Antivirus

DLP solution has to be present on endpoints with central management which prevents sensitive data leakage from endpoints. This not only prevents insider threats but also prevents accidental data ex-filtration. DLP agents on endpoints prevent data upload, data transfer into USB devices (not white-listed), and share to network storage. Host based Antivirus solutions do malware detection on endpoints using signature engine and prevents threats by doing user behavior analytics. EDR (Endpoint Detection and Response) is extended form of antivirus where user entity behavior analytics in done on a central server to get a holistic view of security.

Category X data are to be protected by EDR solutions and for Category Y and Z data, antivirus may be placed. DLP is required for all categories of data.

5.3 Enable TLS Everywhere

Enable TLS (Transport Layer Security) for all supported components to defend against traffic sniffing and authenticate identities at both ends of each connection. TLS not only encrypts north-south traffic but also protects lateral traffic between server and database, server to server, micro service to micro service. All components that support TLS should have it enabled and configured properly. For all categories, TLS 1.3 is essential which is having Perfect Forward Secrecy. For Category X, standalone Enterprise Root CA (Certifying Authority) is recommended. For other categories, CCA certificate trust chain may be used.

5.4 Removal of Unnecessary Ports and Services

Removing ports and services that are not in use is an essential practice in Cyber Security and network hardening. Ports that are not in use must be disabled at underlying OS to protect them to be used by an attacker. Services that are no longer to be used has to be shut down or disabled so that no loop holes are left. By minimizing the attack surface and reducing potential points of entry, organizations can significantly enhance their network security.

5.5 Hardening of Endpoints

Hardening of Endpoints can be done only for those endpoints that are either managed or kept inside organization's premise. For all categories of data these endpoints are to be hardened. Hardening of endpoints is highly dependent on the host OS that implements the Transport Layer. The minimum hardening of Windows based endpoints includes following:

- End points should be on a domain controller such as Active Directory
- Revoking Admin privileges
- Renaming Admin Accounts and disabling Guest accounts
- Setting up account lock out policy and password age
- Disabling of Power shell and Command Prompt
- Basic Input Output System (BIOS) should be protected
- Disk Encryption should be enabled

5.6 Endpoint Security Posture Check

Category Y and Z data are available on unmanaged endpoints. These unmanaged endpoints can't be hardened but a posture check is done with the help of endpoint posture check solutions [12] before these devices are connected to the organization's network. This posture check is a pre-connection check to ensure if the device is following the BYOD policies set up by the organization. In case of violation, connection is denied. Following minimum checks are done as a part of security posture validation.

- Windows Firewall is running or not
- Antimalware and Anti-Phishing is installed
- PUA (Potentially Unwanted Application) including Key Logger and Screenshot capture are not present
- Presence of DLP solution
- Minimum OS version and patch check
- Presence of Blacklisted applications like Torrentz, AnyDesk, Ammyy Admin, Team Viewer

6. SESSION AND PRESENTATION LAYER SECURITY

These layers form the basis of look and feel as well as encrypting the data in transit. The encoding and decoding takes place at Presentation Layer and the Session Layer does the job of opening a dedicated session for an authenticated user. Following approaches are considered to enhance security at these layers:

6.1 Virtual Desktop Infrastructure

In the proposed approach, VDI (Virtual Desktop Infrastructure) is placed at Session and Presentation Layer to explain the security provided at these layers. VDI implements virtual desktops and separate user device from desktop. Use of VDI agents on user device enables users to connect to the resources hosted in data center using their own devices that follows BYOD policies as discussed in previous section. User device is only having a VDI agent that allows the user to acquire a desktop on the fly, known as virtual desktop. The virtual desktop sits inside the data center and not on the user's device. The desktop is non-persistent in nature which means user data will neither reside inside the virtual machine in data center or nor on the user device. As soon as user logs out, data persists in database servers only. Category Y and Z data is allowed over VDI based infrastructure and no downloading is allowed on end user device. As per the need organization can enable the downloading of Category Z data only and that too in encrypted form in white listed USB devices governed by VDI Agent. Each VDI solution is having a VDI security gateway that does endpoint security posture check before allocating virtual desktop to the user. At this layer, MAC address and IP address of the end user device can be considered for additional security. In addition to this, VDI transmits only display data using its native display protocol that can be encrypted by addition TLS layer [10].

Both category Y and Z data are exchanged over VDI channel secured using TLS 1.3.

6.2 Use of SSL VPN

SSL (Secure Socket Layer) VPN works at presentation layer but utilizes the security of Transport Layer. SSL is now renamed to TLS and is now providing host to host security. SSL VPN is an addition layer of security that provides a secure tunnel between end user device and VPN server placed inside organization's premise. SSL VPN can run on a Next Gen firewall as well as a dedicated VPN server can be deployed. VPN hides the actual IP addresses used for communication as well as encrypts data in transit. Category Y and Z data are handled on unmanaged terminals that are protected by end to end SSL VPNs that is overlaid over VDI encrypted channel. Both VDI channel encryption and organization provided SSL VPN use TLS 1.3 security.

6.3 Masking and Limiting Data during Display

Sensitive data are required to be masked at the time of rendering on a display device. The goal of data masking is to protect sensitive data by replacing original characters with special, fictional or scrambled characters/text. This data includes the Personally Identifiable Information (PII) like Aadhaar Number, PAN Number, Bank Account Number etc. All kind of PII information are required to be masked on the screen to prevent the data exposure.

In addition to masking, a limit on maximum number of records in the response to a query may be put in place.

7. APPLICATION LAYER SECURITY

Application Layer is the top layer of OSI model that consists of the actual resource being used by end users. It consists of Web Applications hosted in a data center environment and the browser inside virtual desktop or managed terminal. Most of the tools and technologies that do analytics, central management and provide holistic view of security work at Application Layer which includes SIEM, Honey Pots, PIM/PAM etc. But these tools take help of other layer devices to take information for doing remediation.

Following security posture are considered to implement security at Application Layer:

7.1 Use of Latest and Secured Libraries

Application Layer involves extensive use of libraries that may include proprietary and open source packages and binaries. These should be the latest one and are found to be secure. Any insecure dependency is to be immediately removed. As far as possible, standard functions and libraries are used rather than writing custom codes. Any library or package that has been declared as vulnerable should also be removed at earliest.

7.2 Encryption Using Application Stack

Encryption at application layer is implemented using crypto libraries available in the technology stack used to build the application provides an additional layer of security that also protects data at rest. Since TLS provides encryption of data in transit only, data should be additionally encrypted at Application layer. It ensures that data will remain encrypted at rest inside databases, files etc. This will also keep data protected on components that do not support TLS security. For all categories of data, application should use latest cipher suite:

- AES 256 in GCM mode [5] for encrypting data in transit and at rest
- RSA 4096 for public key cryptography
- SHA3-256 for more secure cryptographic hash
- PBKDF2 for securely deriving cryptographic keys from passphrases in absence of security vault.

All categories of data are to be secured using above cipher suite that is state of the art as on date. With change in time, cipher suite has to be upgraded with newer algorithms for better Cyber Security. For category X and Y data, use of security vault and key management system is recommended for storing secrets.

7.3 Secure Coding Practices Using GIGW 3.0 and OWASP Guidelines

Security must come throughout the code development process so that application in itself is robust in terms of security. Secure coding practices are followed by mitigating vulnerabilities and improving Cyber Security posture against popular web-based attacks. Guidelines for Indian Government Websites (GIGW) 3.0 [2] are now having a chapter for Cyber Security unlike earlier versions of GIGW that are followed while building secure web applications. Open Worldwide Application Security Project (OWASP) [1] is also continuously updated against various web-based vulnerabilities and popular attacks, using which a web application is made robust in terms of security. Websites handling all categories of data has to follow these secure coding practices mentioned in these guidelines.

7.4 Use of SIEM

SIEM (Security Information and Event Management) is a solution that works at the Application Layer but complements SOAR (Security Orchestration and Response) to take remediation action at various layers using devices that work at their respective layers. Use of SIEM is done to monitor and analyze logs generated by different components such as routers, switches, databases, applications, firewalls, virtual machines, hypervisors, PIM/PAM etc. to get a holistic view of security and mitigate zero-day attacks. SIEM collects and analyzes log and event data from various sources within an organization's IT infrastructure to provide real time insights into security threats, incidents and overall networking activity. Few of the major features provided by the SIEM include log and event correlation, incident investigation, real time monitoring, and UEBA (User and Entity Behavior Analytics). Using some cyber security frameworks such as MITRE attack, SIEM can analyze attackers' strategies and techniques and can throw alerts on predefined set of rules. This is done to prevent zero-day attacks. The centralized placement of SIEM in an organization provides a holistic approach to enhance the security landscape [6] [7].

Category X and Y data are handled in an environment supported by SIEM based monitoring. Category Z data handling may avoid the use of SIEM. Regular processing of Cyber Threat Intelligence received from OEMs and Organizations such as CERT-In is to be done and action to be taken based on the alerts generated by SIEM to protect each category of data. Use of SOAR to implement a state-of-the-art SOC is highly recommended [8] that automate the incident response.

7.5 MAC and IP Address Binding

MAC address and IP address of endpoints are to be bind/linked to each other and validated at Application Layer to prevent unauthorized devices to access the application using unmanaged terminals. Managed terminals are already taken care of by MAC binding done at switches or firewalls that are managed by organization itself. MAC and IP binding prevents changes in the IP address of a particular endpoint. In other words, at Application layer a database can have a list of pre-approved list of MAC and IP addresses that can access application. Applications handling all categories of data are required to have MAC and IP address binding implemented.

7.6 Use of PIM/PAM to Control Access

Use of PIM/PAM (Privileged Identity Management/Privileged Access Management) to manage critical resources like servers, databases, Kubernetes clusters, Applications etc. is required to prevent insider threats. Use of dedicated terminals is required to support PIM and PAM solutions by authorized users to gain access to all critical resources such as firewalls, router, switch, Application server, database server, etc. Direct access to any of these resources should be prevented by physical safeguards. This will set the accountability of the team managing these resources and prevents insider attacks. Although PIM/PAM work at Application Layer but it is used to access almost every device working at different layers of OSI model. This also includes the management of managed terminals.

Infrastructure handling Category X data are to be managed under PIM/PAM based environment. Category Y and Z may avoid the use of PIM/PAM. Since PIM/PAM do not restrict the direct physical access to the assets, any access outside the purview of PIM/PAM can be made as a rule under SIEM to generate appropriate alerts.

7.7 Deployment of Honey Pot

Deployment of Honey pot to understand your security landscape as well as hacker's strategies with respect to your infra is an advanced security defense practice for critical infrastructures. Honey pots are a cyber security tool and technique used to deceive and detect malicious actors by creating controlled and monitored environments that mimic real systems, applications, or networks. The primary purpose of honey pots is to attract and divert cyber attackers away from actual critical assets while allowing security professionals to observe and study their tactics, techniques, and procedures (TTPs). Honey pots can be valuable tools for threat intelligence, incident response, and understanding evolving cyber threats. Decisions of Honey Pots are up to the organization's venture into security defense mechanism as it needs to mimic the actual infra as closely as possible and involves lot of cost. In the proposed approach, no category is mapped to the deployment of a honey pot.

7.8 Web Application Firewall

Deployment of Web Application Firewall (WAF) is a firewall that works at Application Layer to protect web applications from several web attacks such as SQL Injection, Cross Site Scripting (XSS), Brute Force Attacks etc. WAF can protect Web Server and Applications by doing behavioral analytics, signature-based detection at the layer, IP Reputation, Rate Limiting and Geo-location Blocking. For all categories of data, WAF is recommended to be placed in front of Web Server processing data.

7.9 Sandbox

A Security Sandbox refers to an isolated and controlled environment where software and processes can run separately from the rest of the system. Any media being uploaded into an IT system or being downloaded from external source is first allowed to execute in a Sandboxed environment just like it runs on production system to find out the threats and vulnerabilities, if any, present in the media so that it is first sanitized before ingestion into the actual system. Other important scenario for which usage of a Sandbox is recommended includes Security Testing of malicious & untrusted software and Dynamic Testing of Applications in a controlled environment.

Systems processing Category X data are highly recommended to have Sandbox environment to sanitize data being ingested into it.

8. OTHER COMMON SECURITY MEASURES

Some of the common security practices that are generic and applicable to multiple layers include following:

- Use of MFA (Multi Factor Authentication) is to be done wherever possible. All categories of data are to be handled using MFA enabled at various layers.

- Strong password at each level that includes network devices, VMs, Hypervisors, Applications, databases etc. It should meet minimum length and pattern complexity. Removal of default passwords everywhere.

- Security Audit on regular intervals. It includes process audit and VAPT (Vulnerability Assessment and Penetration Testing) of ICT infra. Periodic Penetration Testing is recommended for organizations handling Category X data while all three categories must undergo periodic Vulnerability Assessment.

- Logs generated by servers, endpoints and application servers are to be kept protected. Category X data demands encrypted logs that can't be tampered. Retention of logs is to be governed by organization's policy.

- Principle of Least Privilege to be followed at each layer.

9. CONCLUSIONS

The Cyber Security of data is a continuous process that is required to be handled with a holistic approach. There is no fit-for-all kind of solution that is used to protect different categories of data based on their sensitivity. Since the Cyber Attacks are happening at every layer of an OSI model in an IT system [14], the security landscape must include a robust security posture considering each and every layer. Cyber Security should come by design of IT environment where classification of data is done based on its security sensitivity and mappings of assets are done as per the security classification label. This not only enables protection of data in a robust way but also strikes a balance between reliance on managed and unmanaged infrastructure, thus reducing cost of operations.

REFERENCES

[1] https://owasp.org/www-project-top-ten

[2] https://guidelines.india.gov.in/introduction/

[3] Elina Battaglia, Livio Bioglio, Ruggero G. Pensa. 2020. Classification-based Content Sensitivity Analysis. SEBD 2020. CEUR Workshop Proceedings. 326-333.

[4] El Ouazzani, Amina & Harbi, Nouria & Hassan, Badir. (2016). Dynamic Classification of Sensitivity Levels of Datawarehouse Based on User Profiles. International Journal of Database Management Systems. 8. 13-25. 10.5121/ijdms.2016.8602.

[5] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[6] Granadillo, Gustavo & González-Zarzosa, Susana & Diaz, Rodrigo. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 21. 4759. 10.3390/s21144759.

[7] A. Vazão, L. Santos, M. B. Piedade and C. Rabadão, "SIEM Open Source Solutions: A Comparative Study," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-5, doi: 10.23919/CISTI.2019.8760980.

[8] https://www.ibm.com/topics/security-orchestration-automation-response

[9] Scott Rose, Oliver Borchert. (2020). Zero Trust Architecture. NIST Special Publication. 800-207.

[10] https://www.vmware.com/topics/glossary/content/virtual-desktop-infrastructure-vdi.html

[11] Olalere, Morufu & Abdullah, Mohd & Mahmod, Ramlan & Abdullah, Azizol. (2015). A Review of Bring Your Own Device on Security Issues. SAGE Open. 5. 10.1177/2158244015580372.

[12] https://www.opswat.com/products/endpoint-security-sdk/device-compliance

[13] David Kuipers, Mark Fabro. (2006). Control Systems Cyber Security: Defense in Depth Strategies. Idaho National Laboratory. INL/EXT-06-11478.

[14] https://www.byos.io/blog/types-of-cyber-attacks-osi