Journal of Software Engineering and Applications, 2016, 9, 601-623
http://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach

Joseph E. Mbowe[1], Simon S. Msanjila[2], George S. Oreku[3], Khamisi Kalegele[1]

[1]School of Computational and Communication Science and Engineering, The Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania
[2]Faculty of Science and Technology, Mzumbe University, Morogoro, Tanzania
[3]Faculty of Economics, North West University, Vanderbijlpark, South Africa
Email: mbowej@nm-aist.ac.tz, khamisi.kalegele@nm-aist.ac.tz, simon.msanjila@mzumbe.ac.tz, george.oreku@tirdo.ac.tz

How to cite this paper: Mbowe, J.E., Msanjila, S.S., Oreku, G.S. and Kalegele, K. (2016) On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach. *Journal of Software Engineering and Applications*, **9**, 601-623.
http://dx.doi.org/10.4236/jsea.2016.912041

Received: July 9, 2016
Accepted: December 27, 2016
Published: December 30, 2016

Abstract

The integration of organisation's information security policy into threat modeling enhances effectiveness of security strategies for information security management. These security policies are the ones which define the sets of security issues, controls and organisation's commitment for seamless integration with knowledge based platforms in order to protect critical assets and data. Such platforms are needed to evaluate and share violations which can create security loop-hole. The lack of rules-based approaches for discovering potential threats at organisation's context, poses a challenge for many organisations in safeguarding their critical assets. To address the challenge, this paper introduces a Platform for Organisation Security Threat Analytic and Management (POSTAM) using rule-based approach. The platform enhances strategies for combating information security threats and thus improves organisations' commitment in protecting their critical assets. R scripting language for data visualization and java-based scripts were used to develop a prototype to run on web protocol. MySQL database management system was used as back-end for data storage during threat analytic processes.

Keywords

Security Threats Analytic, Threat Visualization, Security Management, Automated Security Policies

1. Introduction

The security literature has shown that system's users are the weak link for security

breaches [1] and therefore hackers use this loop hole to break the system for their personal gain or otherwise. Despite the user being a weak link, the advancement in computer technology also produces a huge number of data *i.e*. information overload compared to the organisational ability to manipulate in order to extract potential useful information for informed decision-making [2] [3] [4]. According to Mbowe *et al*. (2014), the security awareness and maturity level for selected organisations in Tanzania are not satisfactory in many aspects. For example, about 92.1% responses of respondents indicated that their organisations had no effective strategies for managing their ICT assets in regard to security breaches and only 41.2% responses of respondents were aware of the existing security awareness programs in their organizations. It was noted that, the top management (e.g. directors, managers, supervisors or executive officers exercising the organisation's powers) considers the information security management as a technical issue rather than a business issue, in which there exists little or no close eye from top management to oversee information security compliance. The poor realization of information security as a corporate governance responsibility has promoted the deadly sins of information security management [5]. As a result, it causes the security management imbalances among internal stakeholder due to inadequate security sense and commitment across the organisation structure. In this context, security management imbalance is the phenomenon of uncoordinated efforts among top management and security managers in protecting an organisation's infrastructure and data.

The more computer technologies become the enabler of organisation's business processes then the top management should put in place the mechanisms for security accountability and effective ways for reporting on the protection of information assets to their organisation's board. In order to undertake efficiently such important responsibilities (e.g. close eye security monitoring), top management and security analysts must employ security tools so as to visualize graphically the organisational potential threats such as Spoofing, Tempering, Repudiation, Information Disclosure, Denial of Services and Elevated Privileges. Nowadays, the STRIDE (e.g. acronym for Spoofing, Tempering, Repudiation, Information Disclosure, Denial of Services and Elevated Privileges) require knowledge and high skills for their discovery due to a huge number of data generated by high-tech computers. For more insight, the STRIDE can be elaborated as follows:

- Spoofing: a third party using another user's authentication information, such as username and password to gain access to the system illegally.
- Tempering: the act of modifying data maliciously without prior permission from the owner.
- Repudiation: the act of denying to performing an action without other parties having any way to prove otherwise.
- Denial of services: the act of denying services or resources to the valid users.
- Elevation of privileges: legitimate privileged users elevate their privileges to access services or resources not granted permission.

Generally, the STRIDE modeling technique has been used extensively during systems

development stage to uncover potential vulnerabilities or flaws which may be exploited by an attacker to gain system access illegally. The technique has not yet been fully integrated in post-development and business operations stages for uncovering the existing organisation's potential threats.

It has been noted that, considerable efforts has been implemented globally to protect information, yet the security issues (*i.e.* threats) have remained persistent in both public and business organizations and surprisingly the existing methods for security threat discovery and analysis demand high level of knowledge and expertise to identify successful attacks. Moreover, the information overload (e.g. big data) produced by high-tech computers have posed a new challenge *i.e.* it requires high-tech skills and knowledge for discovering useful information from big data to support information security management. This paper discusses security threat visualization at organisation's context, its prototype design and implementation. The graphical representation of potential security threats allow security managers and top management draw-up informed decisions in security management and also strengthen the personal security sense and information security as corporate governance liabilities. Thus, increase the realization of information security management in the entire organisation. The rest of this paper is organized as follows: Section 2 discusses research problem overview. The System Model and Functional Requirements are discussed in section 3. Section 4 introduces Platform conceptual design and ruled-based approach. It is followed by section 5 which presents an Experimental Prototype and Results. Further enhancement of the prototype is introduced in section 6 and finally Sections 7 gives conclusions.

2. The Research Problem Overview

The information overload (e.g. big data) requires the knowledge and high skills for discovery of potential threats so that we can build organisational risk-register to support information security management by focusing on day to day organisational risks [6] [7]. Despite the challenges in collection and analysis of security data logs; the integration of organisation's information security policies for visual analytic of potential threats for a particular organisation's context has remained unsolved. The top management and security managers should be enabled to examine these huge amounts of data so that they can quickly represent visually the security challenges at their organisation's context. Also, security managers must be empowered by tools and supportive mechanisms for performing properly their daily responsibilities to improve the strategies for information security management. To undergo rigorous visual analytic, the knowledge-based security threat analytic (e.g. rule-based approaches) is fundamentally an essential consideration for effective security management at any organisation. Actually, the adoption of rules derived from organisation's information security policy force the organisation to develop the security policies which can be implemented by system administrators, enforceable by staff regulations and also hold each person accountable for their activities or duties. In other words, the information security policy set controls for provisions of organisation's commitment in protecting its infrastructure

and data.

While the information security policy plays a big role in security management, it's so important to integrate these policies into security analytic processes especially when monitoring white-list against black-list. In so doing, the organisation focuses on its information security policy and system users to investigate and monitor the anomalous events of a given IT asset. To address this problem, our study proposes a Platform for Organisation Security Threat Analytic and Management (POSTAM) using rule-based approach. The proposed ruled-based approach integrate together the STRIDE model and organisation's information security policy into data mining processes such as knowledge discovery, information analytic and information graphical representation.

3. Proposed System Model and Functional Requirements

Our ruled-based approach, adopted the framework for threat assessment based on organisational information security policy as shown in **Figure 1**.

However, for implementation simplicity the framework was decomposed into system architecture as shown by **Figure 2**. This architecture depicts the blueprints or building blocks for probing the lists of managed objects (e.g. computers, laptops and smart devices) and then evaluates their security conformity based on organisation's information security policy. After evaluation of security conformity, reports are produced and shared across responsible person for appropriate action and mitigation. The elaborated specific functionalities of the proposed platform include:

1) Discovery of managed objects: It involves probing of the organisation's network in order to register all IT assets in the organisation. These assets after being collected are subjected into a set of security rules to evaluate the violation of security policies or

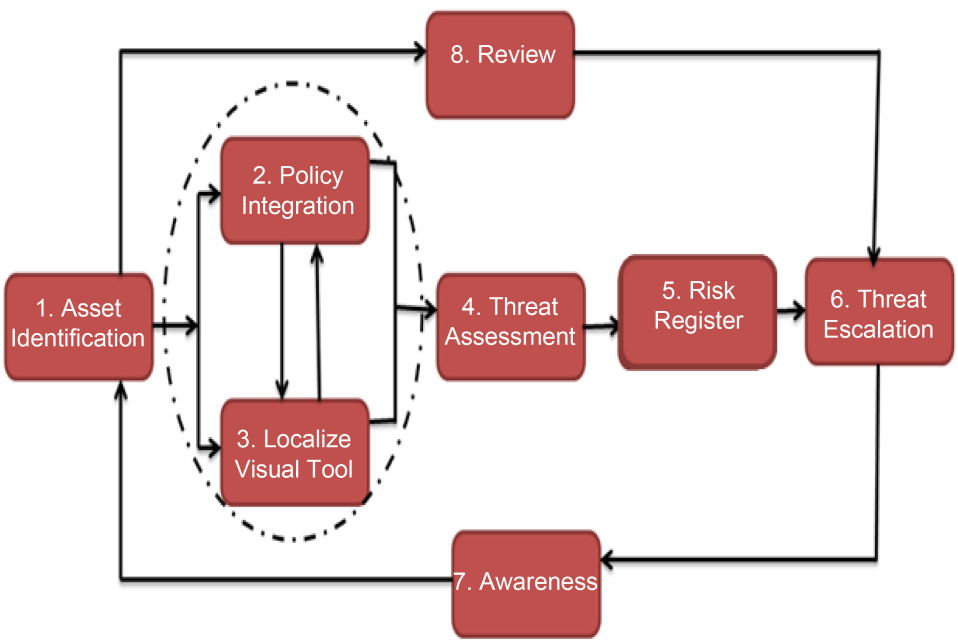

Figure 1. Integrated framework for threat assessment based on organizational policy.

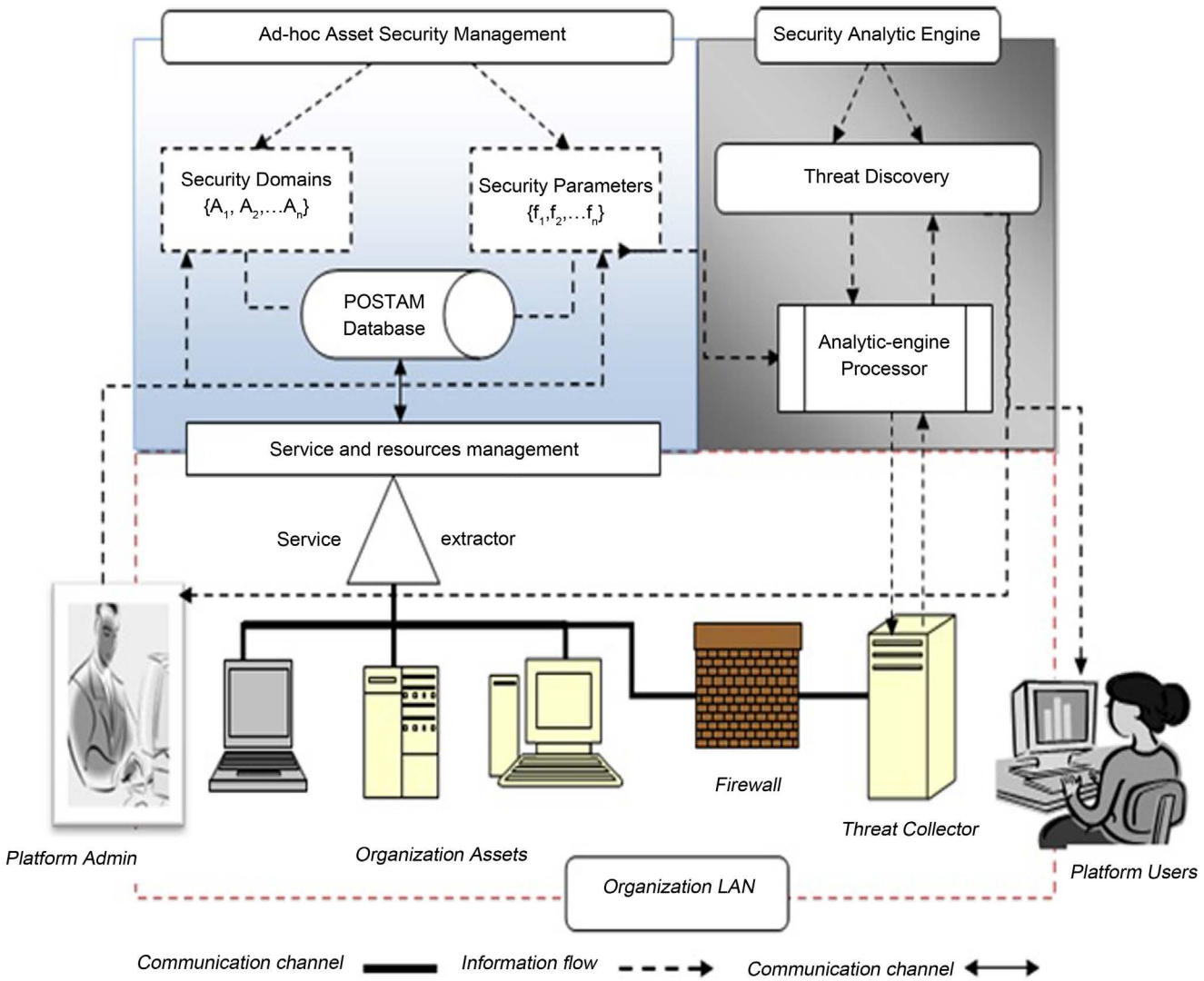

Figure 2. Proposed system architecture.

various attempts for security attacks. In the probing stage, electronic documentation is performed for:

a) Critical assets including owners, location and their running services or resources.

b) Prohibited services and operating rules for a particular group of assets for safer and secure data transmission, processing and storage.

2) Evaluation of policy conformity: A set of rules formulated from organisation's information security policy for each managed object to be evaluated so as to ensure compliance of various security logs, services and human system operations such as:

a) User access rights, prohibited services and un-managed systems configurations.

b) Security audit trail logs and white listing logs.

3) Threat discovery and analysis: After probing managed objects from the organisational network then the information collected from data logs is analyzed appropriately for discovery of potential threats. For example:

a) Collecting system logs files remotely into local machine for easier data mining based on organisation's security context.

b) Transforming system logs into manageable file format for easier data storage and mining.

c) Extracting potential threats from system logs files and store the information for further analysis and report sharing.

d) Building the automated shareable risk-register for quick security monitoring and evaluation.

4) Threat reporting and sharing: The security incidents or events which violate the pre-defined set of rules are shared across organisation's structure as the internal memo for effective information security management.

3.1. Platform System Model

As illustrated by system architecture (see **Figure 2**) and proposed specific functionalities, the following system models were identified. Firstly, Probing Managed Objects (PMO) system model for automatic probing of managed objects including their documentation, running services and data logs. Secondly, the Security Analytic Engine (SAE) system model integrated with information security policy for threat discovery, analysis and storage. By using proposed rule-based approaches, the analytic engine iterates set of security controls against defined security sources (e.g. computer logs and system's user logs) and organisation's risk treatment strategies. Thirdly, the infrastructure system model which represents the Local Area Network (LAN) in which all managed objects operate their day to day business processes. Generally; PMO and SAE system models have various components:

1) Security Domains: the component which describes different security areas for various organisations' managed objects to comply, for example Risk Management, Asset management, Access Control, Security Policy, etc.

2) Security parameters: the set of rules derived from information security policy for provision of security management and thus optimize the security compliance level of each organisational security domains.

3) Client services extractor: the sub-component which extracts all running services from each managed objects using the pre-defined security parameters.

4) POSTAM database: a storage container which stores rules, data or information collected for security threat analytic and management.

5) Threat discovery processor: the sub-component for searching and identifying organisations' threats using rule-based approach.

6) Analytic-engine processor: an engine processor for analysis of organisation's security issues from various security domains.

7) Threat-to-risk processor: a processor sub-component for benchmarking all identified security threats at a given acceptable risk-appetite level and later generate the automated shareable risk-register across organisational structure as internal security memo.

3.2. Requirements Modeling

For system requirements modeling, the Unified Modeling Language (UML) was used to model the system requirements. The UML model tells the users what system can perform (e.g. system specification) and also depicts how the system functioning in a given environment (e.g. system implementation). Also, in software development these UML models have been used to specify the structure and behavior of the system to be built [4]. For example, the question of how actors interact with the proposed platform, we have used the Use Case Diagram (UCD) as shown by **Figure 3** to describe the actors and use case [8] [9]. According to Rumbaugh *et al.* (2014), an actor describes a body or an entity which interact with the system to be developed and the use case describe the transaction among actors and the system. For graphical presentation, the Use Case Diagram for POSTAM is illustrated by **Figure 3**.

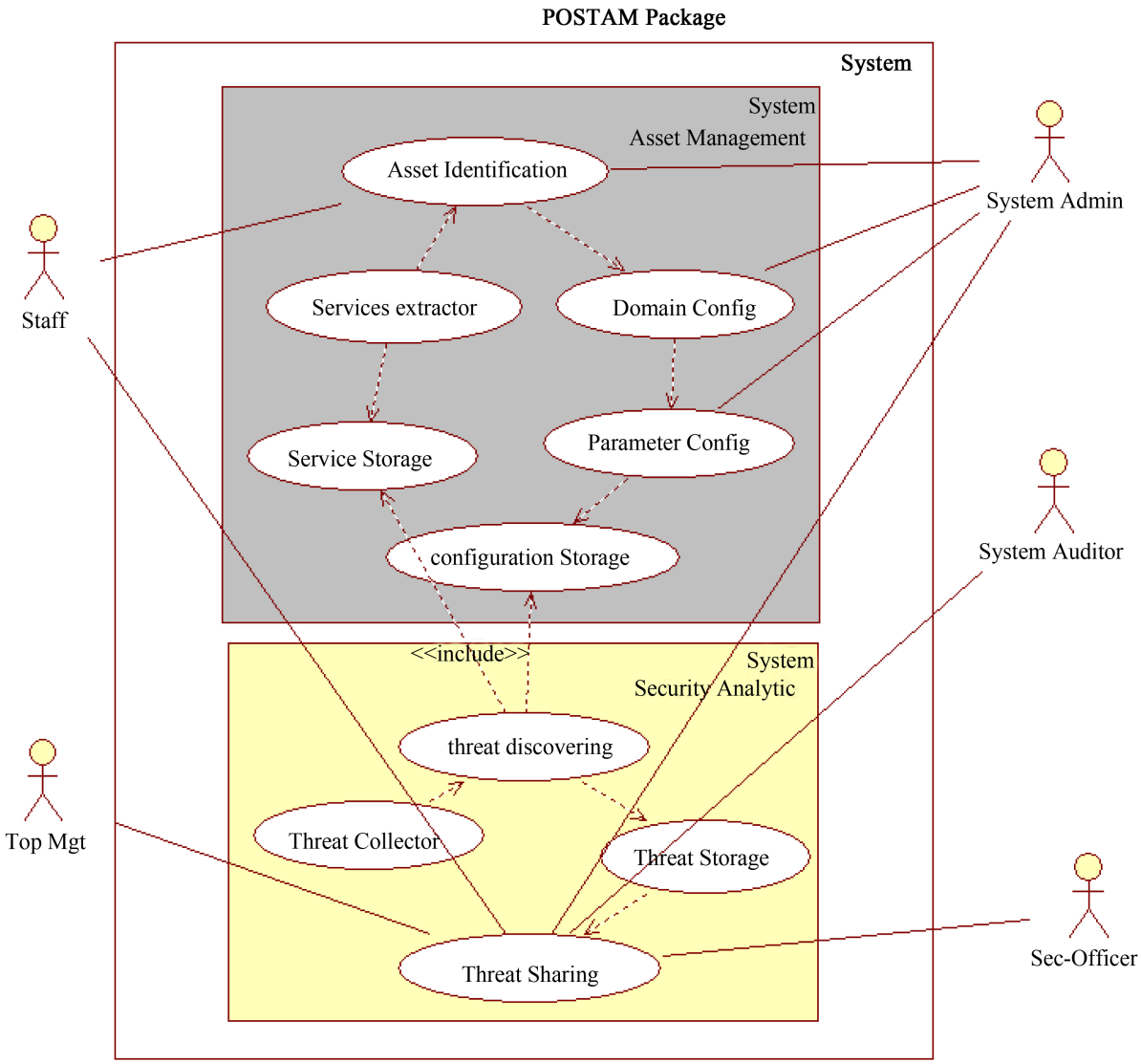

Figure 3. Use case diagram from system interactivity.

3.3. Business Process Modeling

The Business Processing Models was used to describe activities and workflow performed by each system's actors as shown by Figure 4. This activity diagrams show the

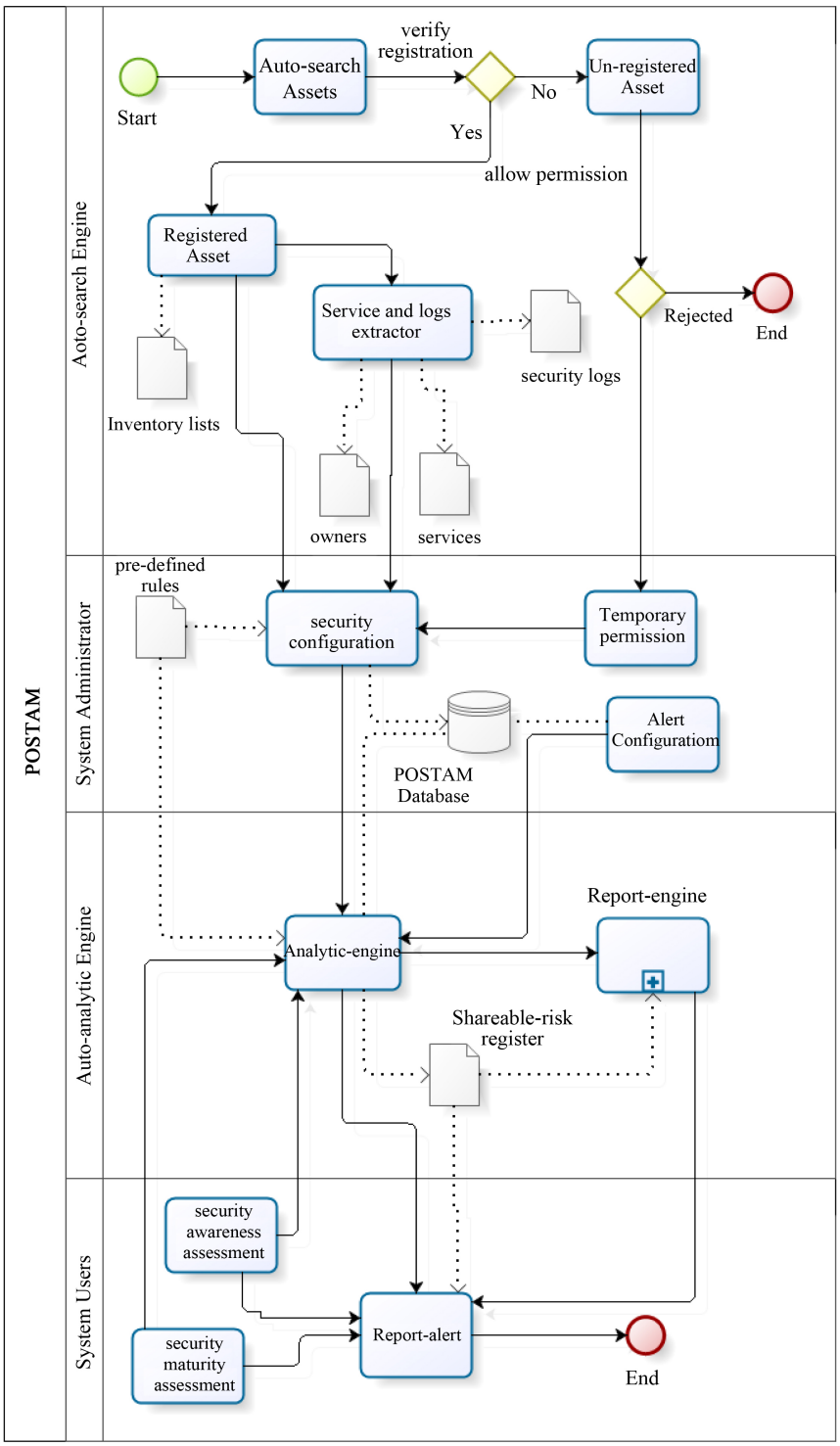

Figure 4. Business process modeling for real-world workflows.

operation sequences including the start and end points of each business activities involved in the security analysis. The proposed major activities include:

1) Probing or discovery of Managed objects: to identify organisation's IT managed objects as essential input for threat analysis. The collection involve updates such as: asset information classification, owner and their locations, running services so as to detect the services which violate the organisation information security policy.

2) Policy integration and administration: for security parameters configurations and user administration with their system's privileges.

3) Threat Analysis: integrates rules for detection the violation of necessary security policies against each identified assets and thus provide necessary information for effective information security management.

4) Alerts and reporting: to share any risky information across the organisation structure for immediate action and mitigation.

3.4. Component Diagram for Packaging Deployment

The component diagram as illustrated by Figure 5 was used to describe different components and to depict the structure for how the platform may be built or deployed

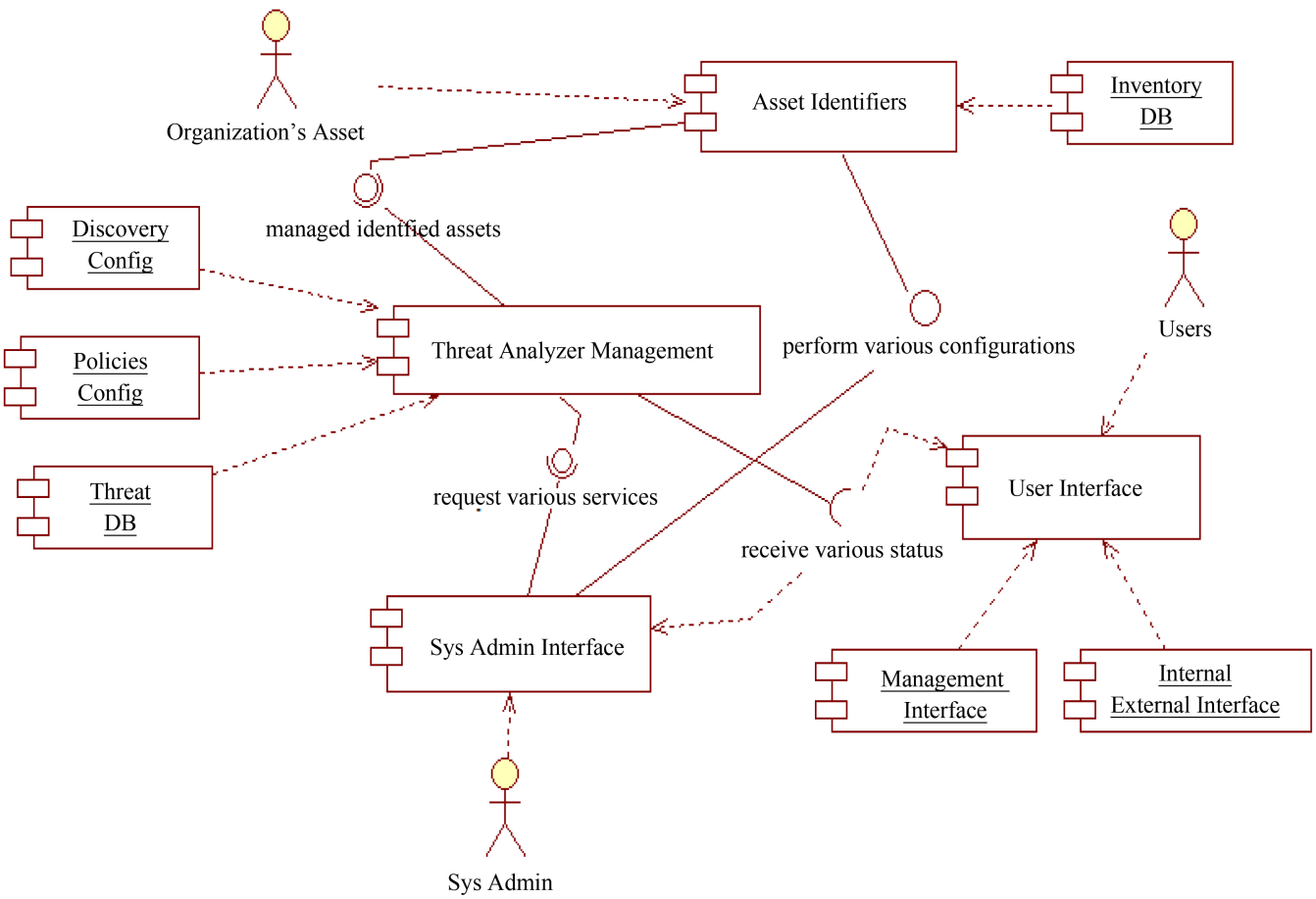

Figure 5. Component diagram for packaging deployment.

including their dependencies. In this case, the proposed platform has two major components with sub-components as described below:

1) Component for Ad hoc Probing of Managed Object for inventory lists including various system administrator and user interface, system configurations, interaction links for database navigation and storage of the inventory list and their associated information for threat analysis.

2) Component for Security Analytic Engine for provision of threat analytic and management based on appropriate information security policies. These analytic-engines include sub components such as:

a) Threat analytic sub-component for analyzing the potential threats and their influential magnitude in the organisation critical information.

b) Threat-to-register sub-component which rates and evaluates the identified security threats to build the automated risk registers to be shared across the organisation structure.

c) Alert sub-component which reports all risk across organisation structure based on pre-defined escalation procedure.

As stated earlier, the platform has two major components with sub-components as described below:

1) Ad hoc Asset Security Management component with various system admin and user interface, system configurations, interaction links for database navigation and storage of the inventory list and their associated information for threat analysis.

2) Security Analytics Engine component for provision of threat analytic and management based on appropriate information security policies. These analytic-engine include sub components such as:

a) Threat analytic sub-component for analyzing the potential threats and their influential magnitude in the organization critical information.

b) Threat-to-register sub-component which rates and evaluating the identified security threats to builds the automated risk register to be shared across the organization structure.

c) Alert sub-component which report all risk across organization structure based on pre-defined escalation procedure.

3.5. Entity Diagram for Database Implementation

In designing the back-end database, the entity modeling techniques were used [10]. We have adopted this technique so as to provide necessary information for systems developers to implement accurately the physical schema to store into database systems the discovered potential threats. In order to avoid data redundancy and implementation of *many-to-many* relational datasets, various entities were identified and normalized appropriately as illustrated by **Figure 6**. For example, we have established entities for:

1) Staff as the owner of information assets including their category, locations and granted information classification to be processed, transmitted or stored on their respective assets.

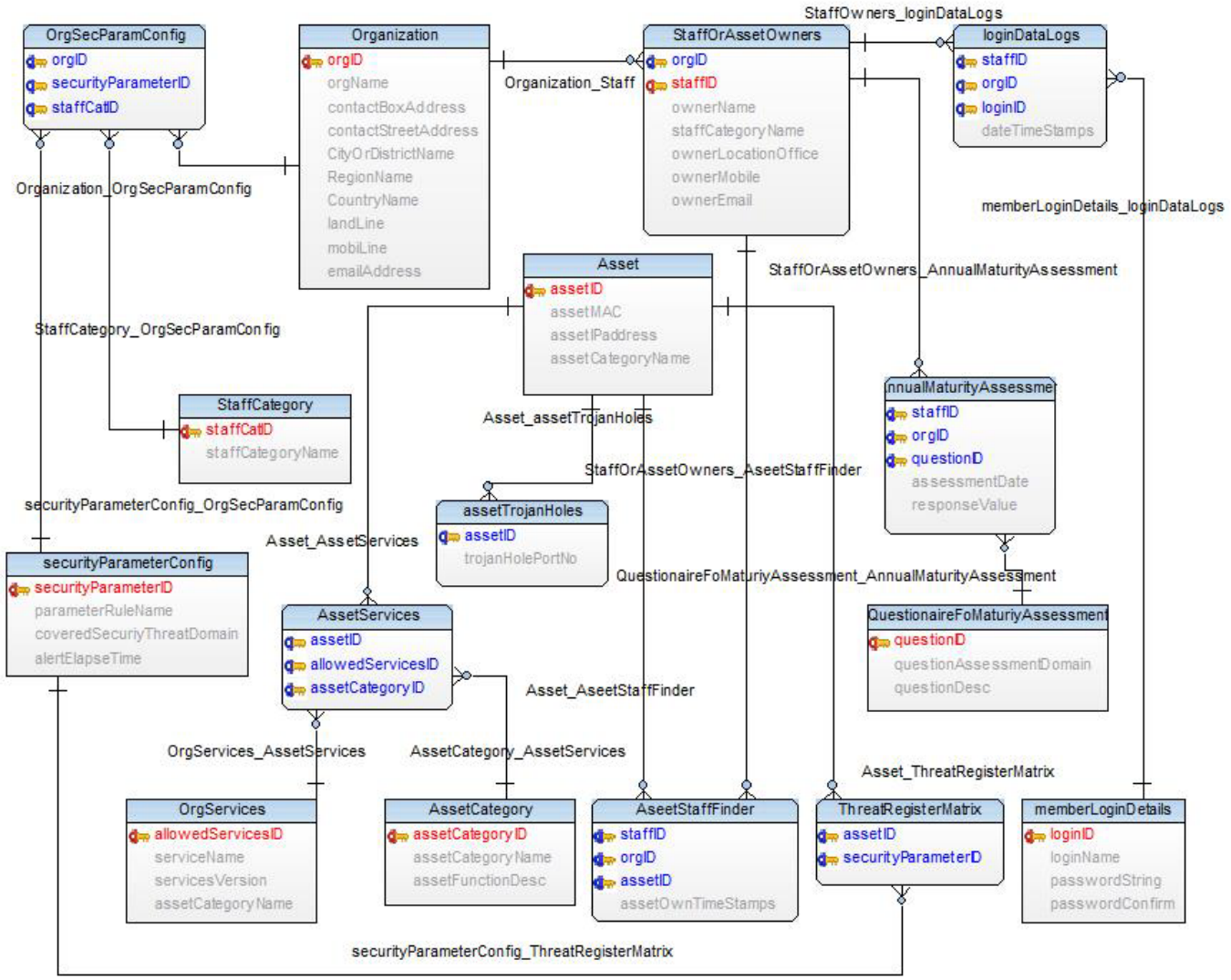

Figure 6. Entity relationship model for database implementation.

2) Asset as the source and target for security breaches including granted information classification to be handled by the respective asset including asset category, running services, prohibited services and active Trojan ports, use-policy configured for this asset etc.

3) Register for registering the collected threats including their sources, impact and check-indicators for integration with organisation security policies.

4) Evaluation questions and their test category for assessing maturity level and security awareness at individual across all ISO 27001 security domains.

5) Likert-type anchors for measuring the extent of threat captured from the organisation's information asset.

4. Platform Conceptual Design and Ruled-Based Approach

Our research selected some ISO domains as shown on Table 1 for deriving initial

Table 1. The selected strategic objectives and controls for security analytic processing.

ISO	Sub-Control	Security Control Objective	Automated Check-Indicators
Organization Policy	Ensure existence of information security based on organization risk assessment criteria	- Establishment of approved information security policy with control objects and commitment at individual and organization levels.	- Assess security awareness and compliance at individual level for all internal and external stakeholders at given time interval - Assess organization security maturity level
Asset Management	Management of critical assets for example their responsibility, associated owners, acceptable use and coding or labelling	- Identify all assets and define its protection appropriately - Allocate each asset with appropriate user and use-policy accordingly - Labelling all critical asset and procedure for all management of removable media	- Automatic identification of assets inventory list and associated :use-policy, information classification tags and ownership - Automatic verification of connected removable media in accordance with use-policy - Automated procedure for evaluating security awareness and organizational maturity level
Operations Security	Protection from malware, viruses and potential vulnerabilities	- Protect from malware each transmission, process-ing and storage critical assets - Record and manage all user and system logs - Identify potential technical vulnerabilities	- Automatic alerts for any associated malware processes or activities actively running on protected asset - Automated regularly review of potential known vulnerabilities, system's logs and user activity logs so as to check potential security warning or information
Incidents Management	Analytics of security incidents and weakness identified from each asset and users	- Evaluates security awareness and maturity level across the organization structure - Establishing learning from collected information security incidents and weakness	- Automated analytic engine to analyze security weakness and incidents from each user including all assets owned by such user - By use of Charts and plots demonstrate the identified analytic learning from security incidents, violations and weakness using graphs for easy interpretation without expertise

automation check-indicators and controls including organisation's strategic security objectives in order to operate on that organisation's context.

4.1. Entity Prototype Design Considerations

For our ruled-based approach, four design considerations were identified as follows:

R1: Enabling automated questionnaires provides quick security situational awareness and organisational maturity level. Furthermore, automated questionnaires ensure real-time information about security awareness for each individual in the organisation and thus provide useful information for closely monitoring of security awareness programs and also preparation of appropriate security programme for each identified group (s).

R2: Fusion of organisational policy into managed objects for threat analytic processes provides a practical mechanism for timely verification of white-list against black-list in the organisation. The integration of organisation's information security policy into operations of each managed objects forces the organisation to define appropriately the set of security issues, controls and its commitment in order to protect its critical asset and data more efficiently.

R3: Graphical data visualization provides simple and intuitive mechanism for direct interaction of anomalous activities of a particular managed object. It simplifies the ability for gathering and processing knowledge representation for informed decision-making by top management.

R4: Sharing security related reports as an internal security memo strengthens the strategies for information security management. The web-based approach increases the robustness for visual data sharing, presentation and analysis.

Based on these design considerations rules, we propose a user-interface as shown by Figure 7.

4.2. Ruled-Based Data Mining and Visualization

The proposed ruled-based approach involves various stages for data processing. These stages include: *input*, *processing* and *output* as illustrated by Figure 8. Each stage is described as follows:

Input: A scheme for remotely collection of security logs and user assessment for security awareness was proposed. For example, we collect security logs from various computers attached to the organisation's network for threats analysis. Also, there exists an automated questionnaire for assessing security awareness for each personnel in the organisation. After collection of security logs and the security awareness data, these data inputs are assembled and stored into appropriate data format for easier analysis and discovery of potential useful information for security breaches.

Processing: The probed managed objects, security system logs and running services for each managed objects are collected remotely in order to *explore* any violations against operating rules (e.g. set of security controls). The analytic engine iterates all system logs and running services against these operating rules to ensure compliance. Incase non-conformity is observed; the report is generated and shared as internal security memo across organisational structure for prompt action and mitigation.

Output: It involves web-based scheme for robust sharing of graphs, charts and customized organisational emerging risks to provide critical information for timely decision-making. For example the following web-interface was proposed:

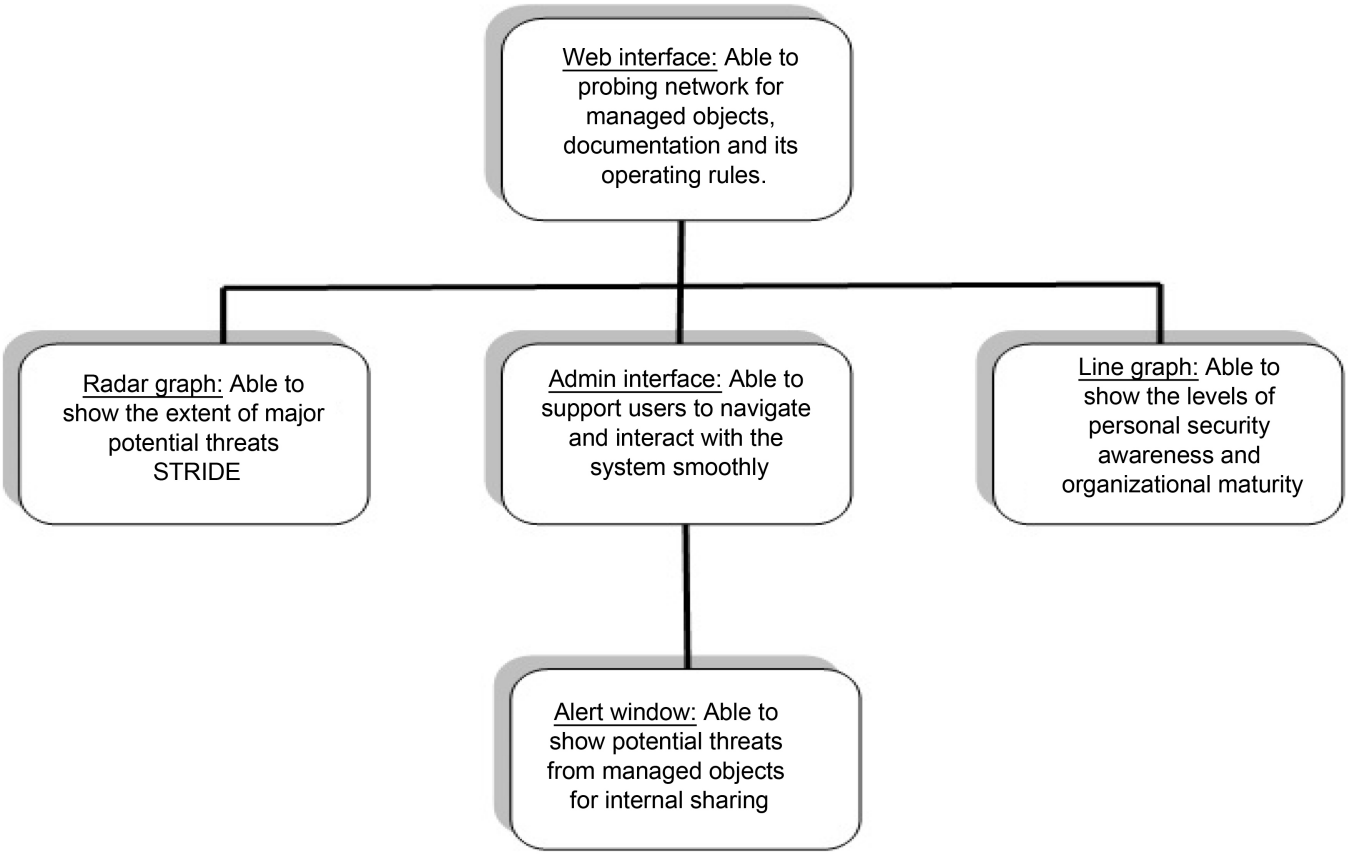

Figure 7. The conceptual interface design model.

1) Risk Alert Page: for automatic sharing of discovered risks or policy violations. Also, this window serves as multipurpose window for user output queries.

2) A radar graph: for visual demonstration of the back-end threats based on pre-defined rules. This graph analyzes possible threats from all critical managed objects including malware activities, logs warning, log-errors, prohibited services, un-managed holes etc.

3) A line graph: for visual demonstration of the security maturity level and security awareness in the organisation. This graph represents graphically all ISO domains by demonstrating the level of awareness and maturity using criteria such as staff or individuals, staff category, quarterly and by given date range.

4.2.1. Proposed Ruled-Based Data Mining Model

Data Mining (DM) has emerged for knowledge discovery especially from big data aimed at predicting the future state of the data for decision making. In so doing, our approach has adopted ruled-based data mining technique for useful information extraction or knowledge discovery (see **Figure 8**) for visualization of organisational security threats from computer logs, awareness data, security maturity data and other security sources or files. From traditional DM process model perspective, we have integrated the STRIDE model and organisation's security policies into the data mining

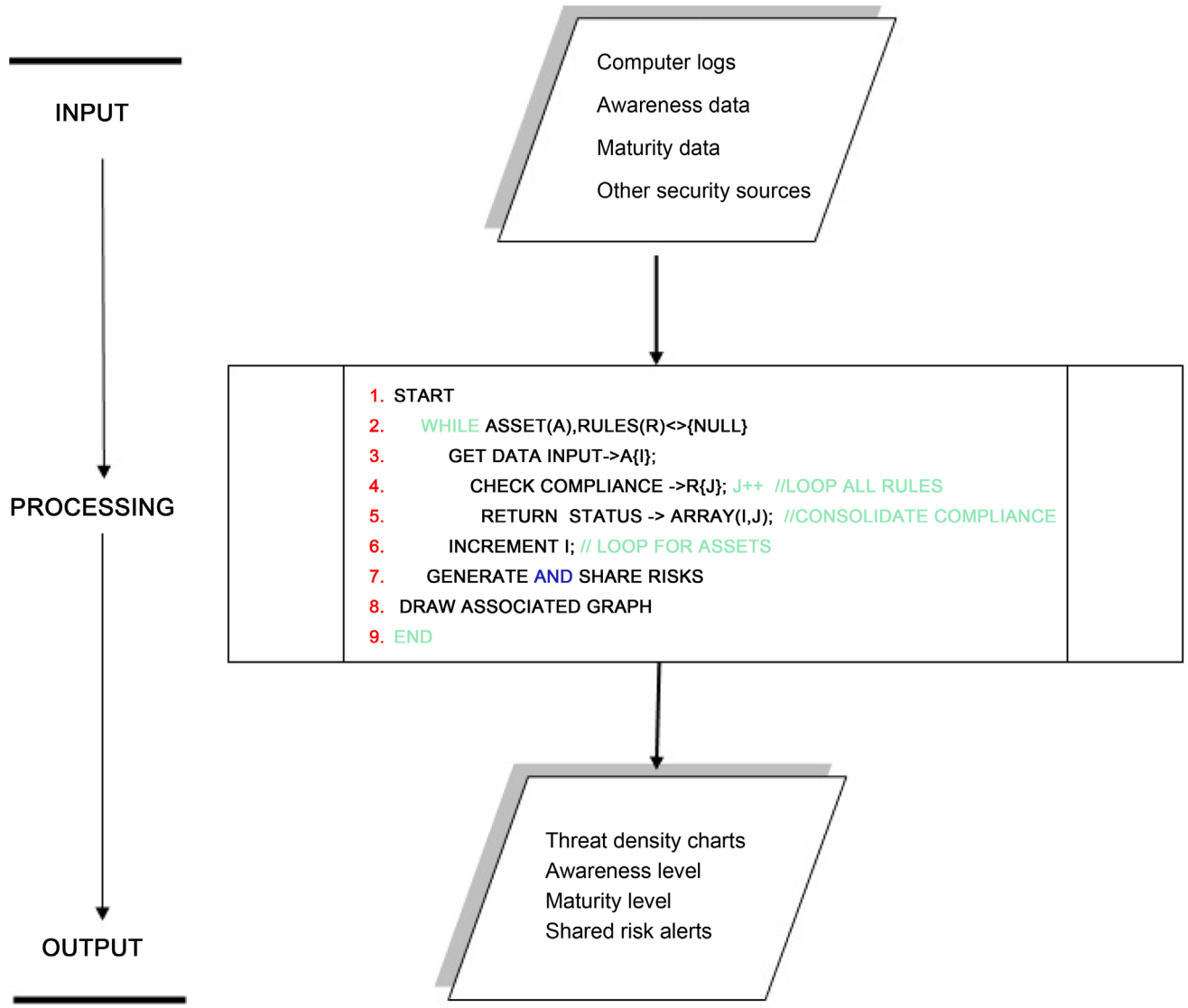

Figure 8. The analytic processing block-diagram.

process model in order to streamline the data mining processes as shown by **Figure 9(a)** and **Figure 9(b)**. By using classification technique; the security log data, awareness and maturity data were classified at different levels of representation or organisational security threats: *spoofing*, *tempering*, *repudiation*, *information disclosure*, *denial of service and elevated privileges*.

To score these organisational security threats, we assessed different levels of the security maturity: *non-existence*, *ad-hoc*, *repeatable but intuitive*, *managed and measurable*, and finally *optimized* as indicated by **Table 2** and later on the organisation's security knowledge and awareness such as *non-existence*, *poor*, *satisfactory*, *good*, *very good* and *excellent*. Furthermore, the Likert-type response anchors [11] with four possible answers—*not at all*, *a little*, *quite a lot* and *completely* with compliance numeric value: −0, 0.33, 0.66 and 1 respectively were used for testing the agreement of com-

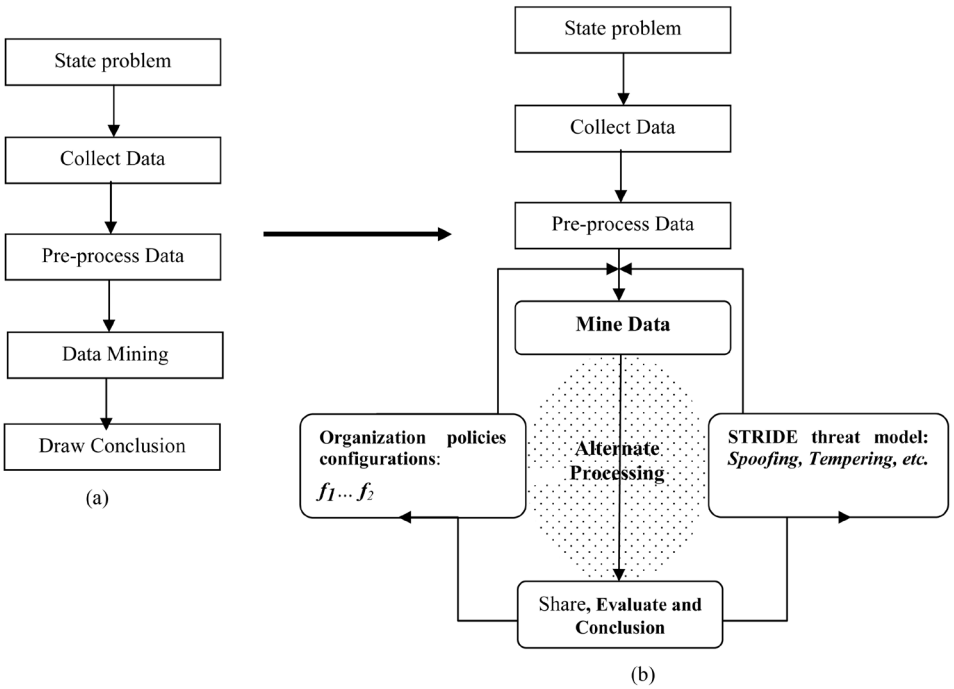

Figure 9. (a) Traditional DM process model; (b) Proposed DM process model.

Table 2. Security maturity and awareness measuring indicators.

Measuring Index	Security Maturity	Security Awareness
0.00 - 0.50	Non-existence	Non-existence
0.51 - 1.50	Ad-hoc	Poor
1.51 - 2.50	Planned	Satisfactory
2.51 - 3.50	Well-defined	Good
3.51 - 4.50	Managed	Very Good
4.51 - 5.00	Optimized	Excellent

pliances of proposed organisation's policies for attainment of appropriate security maturity level and security awareness programs. Also, the conversion by [12], [13] was used to compute the normalized compliances for the purpose of assessing organisation's maturity level and awareness (see **Table 2**). Thus, predicting the potential organisation's threats to be *High*, *Moderate or Low* for numeric values 3.33 - 5.0, 1.67 - 3.32 and 0.0 - 1.66 respectively.

4.2.2. Proposed STRIDE Integrated Policies Data Mining Algorithm

For large data sets, the information extraction using search keys provide a practical way for knowledge or patterns discovery [10]. Our rule-based approach build an array of key-parameters for searching potential threats from formatted datasets collected from security logs of managed objects attached into organization's network. The steps of the proposed ruled-based algorithm are illustrated by **Figure 10**.

Algorithm 1: Event Logs Extraction Algorithm (ELEA)

1: Probe Managed Objects from Organisation network
2: Get security Logs of selected Managed Objects
3: Generate csv or xml logs for information extraction
4: Build arrays of search keys for information extraction (i.e. policies $f_1...f_n$ for security compliance)
5: Given policies $f_1...f_n$ THEN extract information given time-interval
- FOR EACH: policy $f_1...f_n$
  - store dataset-1 onto relational database
  - Generate sorted dataset-2
- From dataset-2 Generate dataset-3 for data visualization or pictorial format.

Figure 10. Event log algorithm for data extraction based on policy.

During integration process, it has been suggested that each asset is integrated by the organization's information security policy so as to operate in specific policies (see **Figure 11**). The selected policies depend on the differentiated services running on such asset to be connected to the network infrastructure of the organization.

5. Prototype Experimentation and Results

After the design phase, the study adopted Web scripting languages and MySQL for web interface and database implementation respectively. The web interface was modeled very simply and intuitively to ensure easy interactivity in security analytic and thus increasing the possibility for wide adaptability across the organisation structure. The organisation V was selected as a case study for experimental prototype implementation. The selected organisation has established ICT policy and its associated ICT information security policy for managing their information assets. However, during data collection we found that its information security policy was based on ISO27001:2005 and thus the controls do not evolve based on organisational risks. Our study adopted ISO27001: 2013 information security management framework which rolls based on organisational emerging risks. However, the controls defined by the organisation's information security policy were used in order to maintain their existing policy structure. After this technical alignment, the data collected [2] during assessment of security awareness and maturity levels were used as pilot data for testing the experimental prototype while on development stage.

5.1. Prototype Experimentation

The functions provided by the prototype were developed using PHP and R scripting languages. The back-end operations (e.g. analytic engine) was implemented by R scripting language (R Core Team 2015) and MySQL database engines. On the other hand, the front-end operations (e.g. web interface for user interactions and data presentation) PHP scripting language was used. The web interface was modelled to be very simple and intuitive to ensure easy interactivity and thus increasing the possibility for

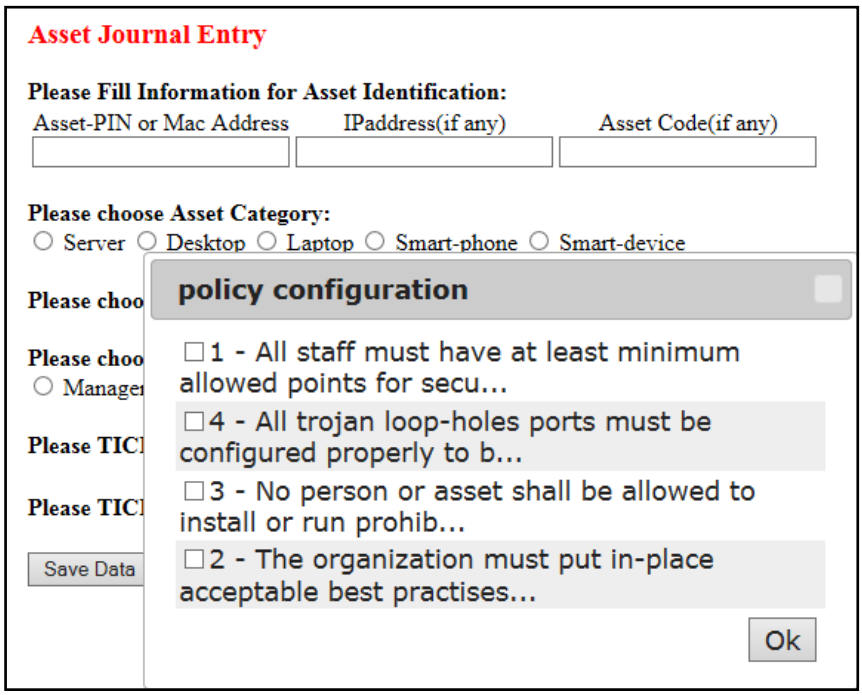

Figure 11. Policy integration for differentiated services.

wide adaptability across the organisation structure. For experimentation purposes, the organisation V was selected as a case study whereby computer logs were collected for analytics and visualization. The output of the prototype is presented by the screen snapshots shown by Figure 12.

Our experiment was interested on Windows Logon Forensics by analyzing different types of logon or logoff activities prompted by a particular event and thus monitoring unusual logon/logoff for *type* 2, 3, 8 and 10. The selected logon types may have high impact on security when window policy configurations are inadequately configured. For example, the check-indicator of each type is described in Table 3.

As shown on Figure 12, the extracted information from window's security logs representing logon/logoff for *type* 2, 3, 8 and 10 is presented by Figure 13.

For evaluation of security maturity and awareness different measuring indicators were used as shown in Table 2. The allocated points lie between zero and five points for minimum and maximum attainment respectively. We used the average point 2.5 to set the benchmark-line for organization to operate in a reasonable good security environment. Normally, all security domains with average zero points indicate non-existence of security awareness. The Likert-type scale; *poor*, *satisfactory*, *good*, *very good and excellent* were used to represent the level of security knowledge. The visualization of maturity and awareness levels based on measuring indicators shown by Table 2 is presented by Figure 14.

5.2. Prototype Overview and Discussion

The data visualization using the proposed prototype has shown that it can be useful for

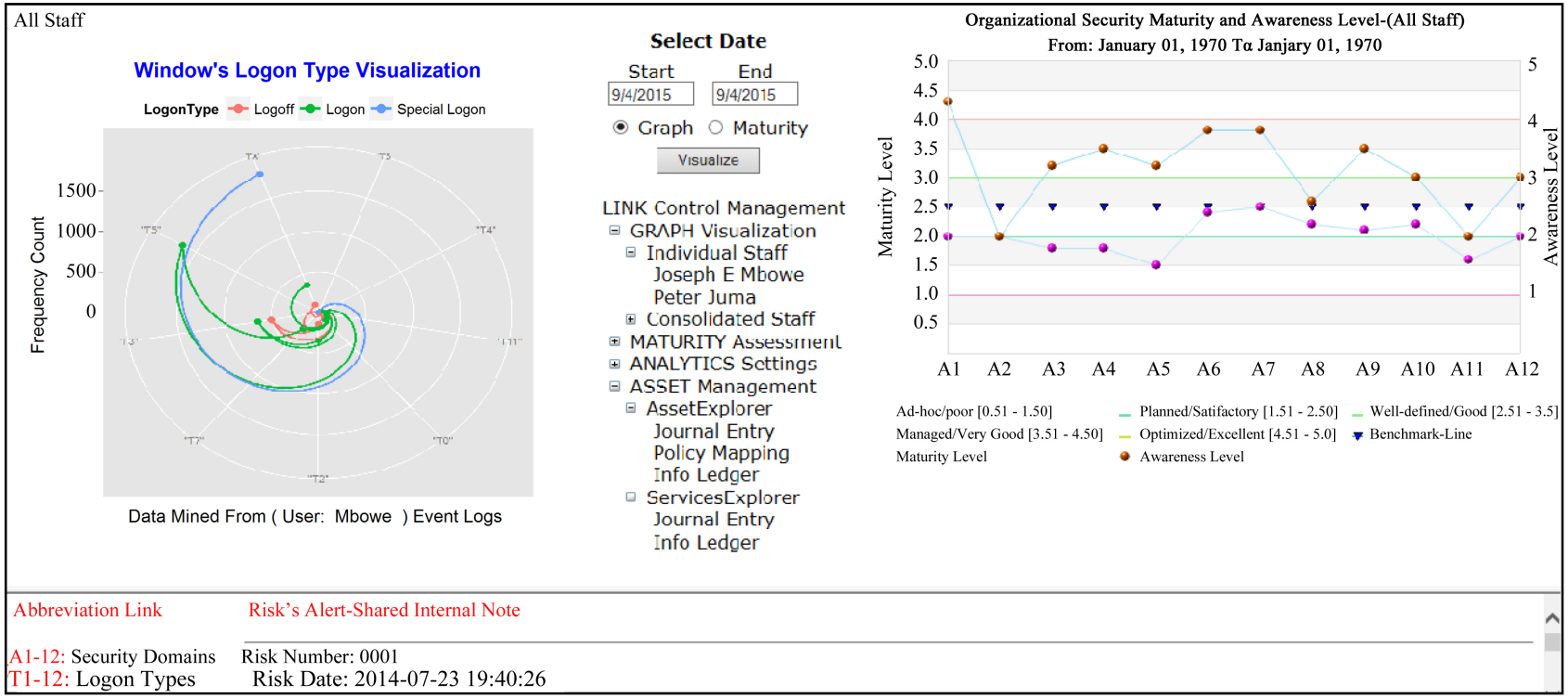

Figure 12. The output graphical representation.

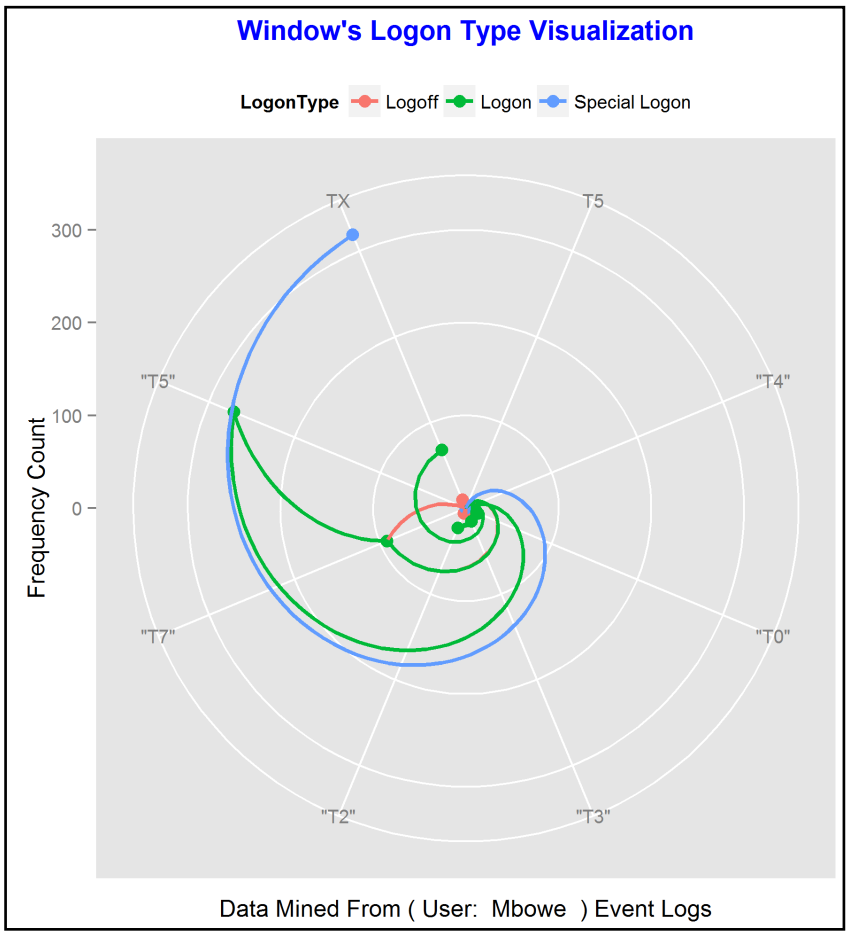

Figure 13. The security log visualization.

leaders, systems administrators and security officers to keep an "eye" on critical systems or computer attached to their cyberspace. Also, the use of pictorial presentation of security logs based on logon types have simplified the visualization of big data such as security logs generated by window security logs. For example, the quick-scan of the summary data showed that about 3% (238) of Audit Failure occurred compared to 97% (7920) of Audit success for a given time interval. Actually, if more Audit Failure occurs, it gives an insight for further follow-up to see what is happening in the background to ensure the success or failure did not occurred due to attack through various security loopholes. Also, the processed information presented by the radar graph (see **Figure 13**) can be used for decision-making in regard to information security management.

Also, the platform has demonstrated the practical ways for automation of organization's information security policy for provisions of effective strategies for security management. It illustrates the extent of the potential inside threats and the user-compliance for a particular organizational environment and culture. Furthermore, it's our opinion that, the greater understanding of the security awareness across the organization structure will be catalyst for management accountability to enhance security management. This proposed platform generate graphs and internal risks notification which

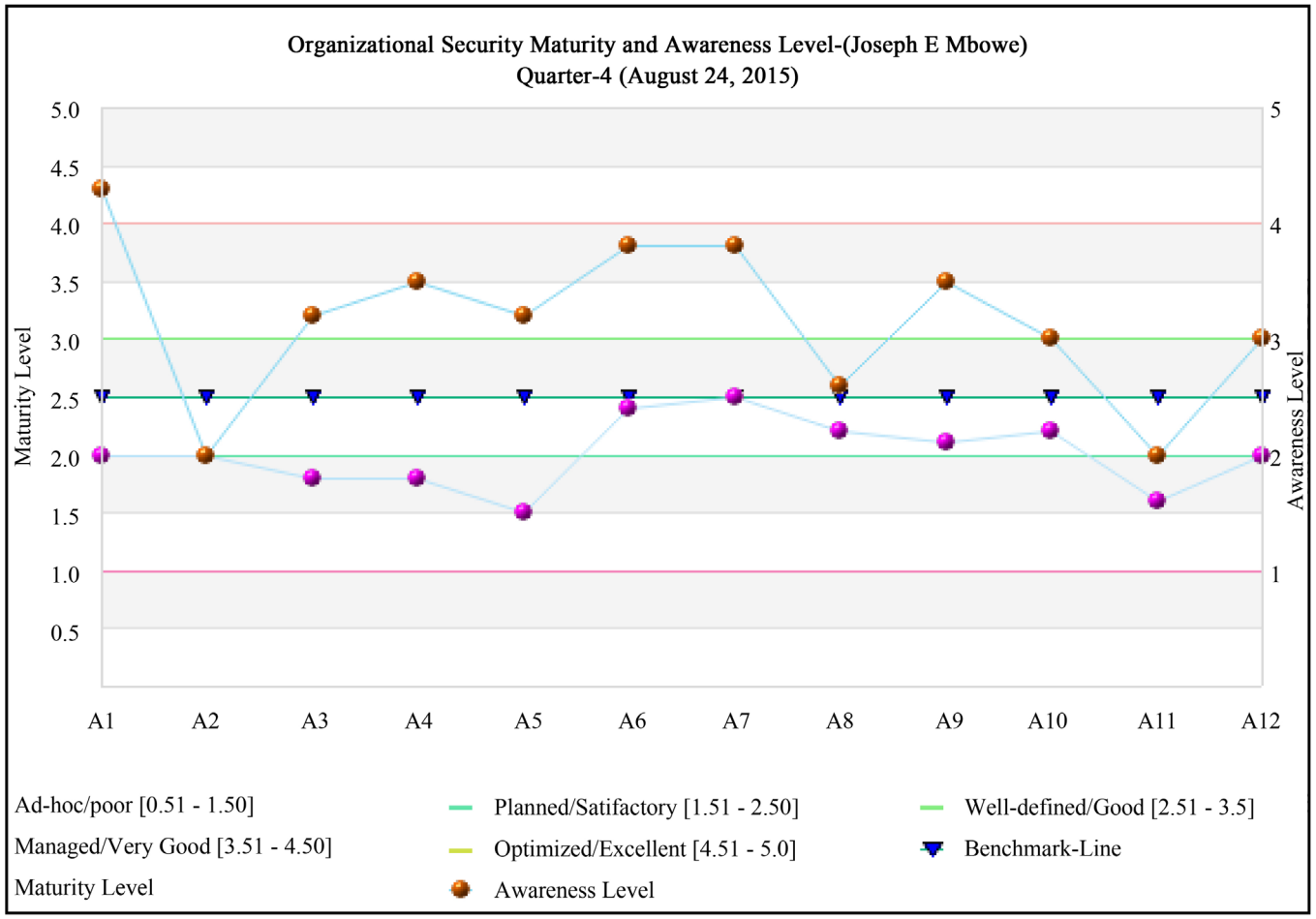

Figure 14. The organizational maturity and awareness level. A1: Risk Management; A2: Security Policy; A3: Organization of Information Security; A4: Asset Management; A5: Human Resources Security; A6: Physical and Environmental Security; A7: Communications and Operations Management; A8: Access Control; A9: Information Systems Acquisition, Development and Maintenance; A10: Information Security Incident Management; A11: Business Continuity; A12: Compliance.

Table 3. Security maturity and awareness measuring indicators.

Logon Type	Description	Check-Indicators
Logon Type 2-(T2) Interactive	A user logged on from console to this computer.	Suspicious Type 2 multiple *audit failure* may indicate password guess or elevation using console or keyboard.
Logon Type 3-(T3) Network	A user or computer logged on to this computer from the network.	Suspicious Type 3 multiple *audit failure* and later *audit success* may indicate anonymous logon by malware or attacker through a network.
Logon Type 8-(T8) Network Clear Text	The user's password was passed to the authentication package in its un-hashed form with audit success.	Type 8 audit success indicate inadequately policy configuration which allows plaintext or clear text as login credentials thus easily to be sniffed.
Logon Type 10-(T10) Remote Interactive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.	As type 3, but user tried to login from remote computer.

can be the source of information for preparing the effective security strategies including security seminars, workshops and training so as to ensure all security domains are well

covered to preserve security confidentiality, integrity, accountability and availability. It was noted that; the prototype was tested based on window's logon audit logs as the subset of security data logs and thus proposing further tests to include various domains of security data logs.

6. Further Enhancement of the Prototype

Currently, the prototype includes threats associated with violation of organization information security policy which was based on ISO27001:2005 security domains and sample data loaded for STRIDE threats evaluation. However, the further work is required to review the existing policy to comply with ISO27001:2013 and also to integrate the automatic assessment of vulnerabilities from security logs and known loop holes associated with malware activities, unmanaged configurations, active Trojan ports and security logs from big data (e.g. security warning and error logs).

7. Conclusion

The security threat analytics using rule-based approach is fundamentally essential consideration for effective security management at organization's context. This paper addressed the methodology for security analysis and management using ruled-based approach. The study has developed the prototype integrated with information security policies to enhance the security strategies for effective protection of critical assets. The generated radar and line graphs for assessing inside threats and security awareness and maturity level in public organization have provided practical approach for improving the internal security strategies for preserving confidentiality, integrity and availability as core services in security management. During prototype testing, we selected one organization from five organizations U, V, W, Y and Z which participated in the previous study [2]. The graphs generated for visual demonstration have provided evidence that, the policies can be automated to support security management based on pre-defined set of rules. The study expects to include potential threats from real-time assessment of vulnerabilities by providing evidence such as the extent of compliance or violation of information security policy.

Acknowledgements

This research is supported by the Nelson Mandela Institution of Science and Technology under the research grant from the Commission for Science and Technology (COSTECH), Tanzania.

References

[1] Anagement, S., Spears, B. and Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly*, **34**, 503-522.

[2] Mbowe, J.E., Zlotnikova, I., Msanjila, S.S. and Oreku, G.S. (2014) A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. *Journal of Information Security*, **5**, 166-177. https://doi.org/10.4236/jis.2014.54016

[3] Nielinger, O. (2003) Rural ICT Utilisation in Tanzania: Empirical Findings from Kasulu, Magu, and Sengerema. Inst. African Stud., Hamburg.

[4] Mijatov, S., Langer, P., Mayerhofer, T. and Kappel, G. (2013) A Framework for Testing UML Activities Based on fUML. *Proceedings of the* 10*th International Workshop on Model Driven Engineering, Verification and Validation Co-Located with* 16*th International Conference on Model Driven Engineering Languages and Systems*, Miami, 1 October 2013, 1-10.

[5] Von Solms, B. and von Solms, R. (2004) The 10 Deadly Sins of Information Security Management. *Computers & Security*, **23**, 371-376. https://doi.org/10.1016/j.cose.2004.05.002

[6] Mataracioglu, T. and Ozkan, S. (2011) Governing Information Security in Conjunction with COBIT and ISO 27001. https://arxiv.org/ftp/arxiv/papers/1108/1108.2150.pdf

[7] Shojaie, B. and Federrath, H. (2014) Evaluating the Effectiveness of ISO 27001 : 2013 Based on Annex A. No. Fares.

[8] Eriksson, H., Penker, M. and Training, O. Business Modeling with UML.

[9] Rumbaugh, J., Jacobson, I. and Booch, G. (2004) Unified Modeling Language Reference Manual. Pearson Higher Education, New York.

[10] Hay, D. (2013) Data Model Patterns: Conventions of Thought. Addison-Wesley, Upper Saddle River.

[11] Vagias, W.M. (2006) Likert-Type Scale Response Anchors.

[12] Pederiva, A. (2003) The COBIT Maturity Model in a Vendor Evaluation Case. *Information Systems Control Journal*, **3**, 26-29.

[13] Krisanthi, G., Sukarsa, I.M. and Bayupati, P.A. (2014) Governance Audit of Application Procurement Using COBIT Framework. *Journal of Theoretical and Applied Information Technology*, **59**, 342-351.