Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

A SYSTEMATIC METHOD FOR MANAGEMENT OF INFORMATION SECURITY ARCHITECTURAL DESIGN AND ISSUES

MUHAMMAD TAHIR
Department of Software Engineering, Superior University Lahore, Pakistan,
Email: msse-f21-016@superior.edu.pk

MUHAMMAD RAHIM ZAFAR
Department of Software Engineering, Superior University Lahore, Pakistan.
Email:msse-f21-018@superior.edu.pk

FAHAD NAZIR
Department of Software Engineering, Superior University Lahore, Pakistan.
Email: msse-f21-017@superior.edu.pk

SALEEM ZUBAIR
Department of Computer Science, Superior University Lahore, Pakistan.
Email: saleem.zubair@superior.edu.pk

MUHAMMAD WASEEM IQBAL
Associate Professor, Department of Software Engineering, Superior University Lahore, Pakistan.
Email: waseem.iqbal@superior.edu.pk

ABSTRACT

Intelligent systems are evolving computer systems based on intelligent approaches that allow continuous monitoring and management of industrial activities. Intelligence improves an individual's ability to make smarter decisions. This study presents a proposed architecture of intelligent systems for information security management. This system intends to enhance security management activities such as monitoring, regulating, and decision-making with an effect size greater than one expert in security by providing techniques to boost the active generation of information about threats, policies, procedures, and risks. Main concern is requirements issues and design for the core components of the intelligent system. There have been several studies that examine management's responsibilities, but none of them have provided a comprehensive picture of what it takes to manage information security. Therefore, managers should research and familiarize themselves with the many responsibilities of management in order to take a more well-rounded approach to information security management. This research investigates the various responsibilities of management in information security and to identify ways in which management may better ensure the safety of sensitive data. The quality of information security management was significantly impacted by a few different management activities. Information security, education, compliance training, corporate information architecture, IT infrastructure management, business and IT alignment, and human resource management were all on the list of responsibilities. So, this study adds to the literature by advocating for a more holistic approach to information security and by identifying actions that managers may do to aid in this area. Many fresh avenues for investigation into the topic have been uncovered by this study.

INDEX TERM: Software architecture, Architecture design, Architecture Issues, Architectural Challenge

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

1. INTRODUCTION

Software architects must consider security while creating systems. Many security issues may be found by analyzing software at various stages (Yu & Le, 2012). Security analysis during design may be done using software architecture design models. Penetration testing, a sort of vulnerability analysis, may be used to test a system for security weaknesses. Architectural security analysis prevents problems from propagating to implementation. Half of all architectural security issues are disclosed (Sametinger, 2013). If we reduce security problems during architectural design, fixing them after implementation will be easier. New architectural styles have been suggested to enable blockchain, microservices, and containerization (Taibi et al., 2018) These architectural styles feature various structures and methods that only tech-savvy individuals can understand (Seifert & Rez, 2016). Security analysis is harder as new styles and technology emerge that software designs adapt. So, analysis must be flexible enough to accommodate new technology and methods. Even if a lot of studies have been offered to aid with architectural security analysis. First, current methods either evaluate design-related security metrics or follow down attack scenarios. Both tasks determine a software's security. The analysis approach should quantify a software system's overall safety for trade-off analysis (Xu et al., 2016). Software developers must be able to determine how security gaps might be exploited and second, most analysis techniques can't be updated to deal with new security metrics or situations since the logic is hard-coded. Third, there are different techniques to analyze architectural style and technology. Information security management ensures that information inside an organization is genuine, kept secret, has integrity, and is accessible. Many factors impact information security management, even if various security solutions aid with different duties. These technologies aren't scalable since they demand constant data analysis. Each security technology offers information in its own manner. Different versions, product lines, and suppliers may not characterize the same symptom the same way. These technologies data can't be analyzed. Analysts in security management must choose the most essential observations (Hosny et al., 2018). A static security technique (safeguard) doesn't provide predictive analytic data. Network administrators or security workers scan databases for vulnerabilities and deploy updates to counter assaults. The technologies used to avoid security issues can't be learn, generalize and adapt with the time. Today’s security solutions lack prediction integration, and real-time feedback to prevent attacks. The technology isn't suited for large-scale assaults. Limitations of each security solution and worsening threats effect information security management and create duties for network managers. Network managers must evaluate a large number of events in near real-time, integrate them, and identify connections. Tracking and identifying sources, detecting and filtering attacks, preventing and preempting them, and so on are all necessary for comprehensive solutions (Chang, 2002). Threat management and security assessment require more automated audits and smart reporting solutions. Real-time threat analysis allows security workers halt attacks before they start. This decreases the harm from successful

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

attacks and reduces the requirement for data recovery and forensic investigation Autonomic computing systems may operate automatically depending on administrator-set objectives. These systems must self-configure, enhance, repair, and defend. Autonomic computing won't operate properly for years. Systems that concentrate on human-agent collaboration are gaining popularity. Security rules may regulate an agent's actions and interactions with humans to ensure it acts in accordance with predetermined guidelines (Bhatti et al., 2004). Security event management systems aggregate threat data from many security and network products, while also minimizing false alarms, linking events from multiple sources, and isolating critical events in order to decrease uncontrolled risks and improve operational security. More automated technologies should forecast security assaults. Auditing and smart reporting systems must aid with security assessment and threat management on a bigger scale, for the past, present, and future. Automated technologies make it simpler to process enormous volumes of data. They make it quicker to gather information from numerous systems, reducing the likelihood of missed assaults. A good information security management strategy requires real-time capabilities, the capacity to adapt and generalize, and the ability to foresee threats and assist people. (Dowd & McHenry, 1998). Intelligence is the capacity to identify unforeseen assaults and prepare how to counter them (Wang, 2005).

Information security management safeguards data. It regulates how individuals utilize technology and make judgments. Information security management ensures that all company data is accurate, secure, and easily accessible. Distinct security solutions assist with different information security tasks. These technologies can't be scaled because of ongoing data analysis. Many systems monitor events, issues, and symptoms. Each security technique gives information differently. Versions, product lines, and providers may not describe the same symptom. These technologies' data aren't accessible. Security analysts must priorities observations. Static security doesn't provide data for predictive analytics. Administrators or security personnel scan databases for flaws and employ upgrades to block attacks. Security team members regularly analyze system data. Each security solution's constraints and worsening threats effect information security management and provide network administrator’s extra work. Problems include data collection, reduction, normalization, correlation, classification, reporting, and response. Network managers must aggregate and assess a vast quantity of events in near real time. Complete solutions must include attack detection, filtering, source tracking, identification, prevention, and preemption (Chang, 2002). Automatic systems are gaining popularity., security rules may manage how an agent operates and inform a human so the agent follows objectives and boundaries (Bhatti et al., 2004). Security event management systems aggregate threat data from diverse security and network products, eliminate false alarms, and integrate events from different sources to decrease uncontrolled risks and enhance operational security. With greater automation, anticipate security assaults.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

2. BACKGROUND

The advancement of the social economy and the rapid expansion of the power business in have made it simpler to construct the power grid (By, n.d.). Many experts are researching ways to strengthen the link between the electrical grid and the Internet of Things in this networked age. There have been many amazing successes in the realm of the Internet of Things in collecting, storing, and managing massive quantities of data regarding electric power, but the challenge of information security has not been totally overcome. The purpose of this study is to look at the design of power information security terminals using big data analysis and the Internet of Things. Because there is so much mobile information regarding the power grid, this study proposes a framework for a power transportation mobile information security management system. This structure makes it simpler for the system to handle power data by using big data, smart sensors, and wireless communication technologies. According to the results of the experiment, the power information security terminal developed in this study may effectively reduce communication resources while saving money on communication expenses when merging data from multiple dimensions. Residents give the intelligent power system scores of 9.312 and 9.233 for convenience and safety in the user satisfaction survey. Overall, leveraging big data and the Internet of Things to construct power information security terminals will increase power companies' service efficiency and provide a better customer experience. This is founded on the notion that safety is the most crucial consideration.

This work is done to deal with enterprise management information security in the context of global informatization, popularize contemporary business Internet of Things (IoT) management technology, maintain enterprise information security, and offer modern upgrading methods for enterprise management. This study (Tang & Ding, 2021) demonstrates how existing Internet and Artificial Intelligence (AI) technologies may be employed before delving into IoT technology in depth. Second, the enterprise management platform is established, and the needs of contemporary enterprise management are analyzed before proposing the design requirements of system functions and the design of the IoT's information security architecture. A platform for controlling the security of business information is also created. There are four components to this platform: IoT data mining management, equipment management, key management, and database administration. The performance of the security management platform is also evaluated in four ways: concurrency testing, stress testing, data testing, and security testing. According to the study findings, the IoT-based business information security management platform built in this work against the backdrop of AI has excellent functionalities and reliable performance of each module. It is tested for stability, stress, big data quantities, and concurrency, and it passes all of them with flying colors. The average reaction time for concurrent and stress tests is around 0.13 seconds, while the average response time for event entry events is approximately 0.25 seconds. The central processing unit (CPU) is never used more

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

than 20% of the time in any monitoring job. As a result, it has been determined that the IoT-based business information security management platform developed in this study is capable of meeting the day-to-day management demands of organizations. Using AI technology, this study can ensure business information security management and establish a benchmark for future research in this field.

The medical information management system, on the other hand, may effectively raise the pace at which medical and health institutions employ their resources, optimize the management process, and offer appropriate, efficient management techniques (Sun & Bai, 2022). All of these factors contribute to medical and health facilities meeting as many internal and external needs as feasible. Projects involving information management systems at hospitals or other medical institutions, on the other hand, are often inhibited by a high degree of system complexity, a significant number of connected linkages, and ambiguity about what the project requires. This is due to the fact that hospitals and other medical institutions have their unique professional and industrial features, which often manifest as several restricting constraints throughout the development process. For continuing medical institution information systems initiatives, determining the kind of risk and how to assess it is critical so that risk evaluation indicators may be evaluated and appropriate countermeasures can be implemented.

In this case, this research develops a flawless method for recognizing and analyzing risks by concentrating on the risk management of projects connected to the medical institution information system at hospital. It also recommends countermeasures for establishing the information management system. Information technology is rapidly developing, which is producing new issues in information security, such as tracking people's identities in e-learning systems. To address these issues, a model of digital identity (MDI) for e-learning systems was created in this study. The MDI's development has two major goals: first, to enhance people's knowledge of information security and encourage them to behave more securely, and second, to bridge security gaps between students and administrators. This approach (Bhatti et al., 2004) differs from others in that it incorporates planning and feedback to achieve these objectives. In the real world, this technique is employed on the Moodle platform, where a security tool that filters out inactive users was constructed as a software plugin (IUs).

The most significant advantages of the MDI are improved personal information security management and the closure of a security gap, such as the absence of complete administrator control over information flow. The experimental findings validate and demonstrate that the suggested security solution works in practice. Also discussed are potential hazards and risks from insider and external attackers, as well as practical solutions to lessen or eliminate them. Finally, this study should have a significant impact on future academic research, as well as assist us understand more about the information security issues that arise when e-learning systems improve.

For the sake of ensuring security, it is essential to include security into the planning and design stages and to make use of a security architecture that ensures both routine

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

duties and tasks directly connected to security are carried out in an appropriate manner (Korać et al., 2022). The demands of the business in terms of security need to be linked to the aims of the company. We came to the conclusion that the security of an organization is determined by four factors: its governance, its culture, the manner in which its systems are constructed, and its service management. A diverse selection of models has been developed so that the strong points and vulnerable areas of an organization's security system may be identified and investigated. The purpose of this model, which is referred to as an information security maturity model (ISMM), is to determine how effectively organizations are able to achieve their security objectives

3. PROBLEM STATEMENT

When it comes to architectural design, making a decision on which agents to utilize is the single most crucial thing to do. The creation of a variety of agents may be of use to those in charge of managing information security (Norvig, n.d.). The individuals who are in charge of making choices and who are accountable should be the major agents in the system that is now being suggested. People often conceive of an intelligent agent as being a combination of intellect and functioning. When agents look at different combinations of functionality, one of the things they will do is functionality, which some approaches refer to as roles. The majority of people believe that a good agent should be located, autonomous, reactive, proactive, and sociable. This is despite the fact that there has been a great deal of debate on what an agent is and which characteristics are essential. The most significant development that has taken place in the realm of autonomous agents is the introduction of AI. The suggested system is unable to make advantage of real-time hybrid architecture as a result of the complexity of the information security control activities. This is due to the fact that the system is built on combining a variety of intelligent agents of various types. Tasks like as acquiring information, organizing it, and utilizing it to help make choices may be automated with the assistance of intelligent agents. They are also able to contribute to an improvement in the overall performance of a network administrator. The performance metrics, or behavioral success criteria, of an agent should be optimized for the agent's architecture and programming in order to get the best potential results (Norvig, 2003). Other essential factors to take into consideration are how easily agents and systems can be transferred, how stable and robust they are, and how safe they are (Bradshaw et al., 2001). The user should be provided with intelligent elements inside the interface that assist them in deciding what to do and how to accomplish it. manage the procedure for maintaining security. It is not appropriate to base performance indicators on how an agent thinks they should behave; rather, performance indicators should be based on what is required for information security management in the environment. At this point of the design process, it is also essential to define the types of feedback that will be offered for learning, because it is often the item that is most crucial to look at when attempting to determine what the issue is that the agent has to deal with. There is often a distinction made in the area of machine learning between supervised learning and

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

unsupervised learning. The administration of information security encompasses a broad variety of activities; for the greatest outcomes, it is recommended that one of these two approaches be used. Another aspect of the agents that you need to take into consideration is their mobility, or the degree to which they travel within the network. Another factor that will be considered in the design is the applicant's level of expertise working with various information security management responsibilities. A significant portion of the education will begin even before the agent is aware of what it is attempting to learn. The agent picks up new information as it examines how it interacts with its surroundings enhancing the functions that each component is responsible to be accomplished via the usage of a development spiral process. ISISM is designed such that its feature set may be customized to meet the specific requirements of any individual organization. The amount of money that is available and the tasks that need to be completed determine the sequence in which models are implemented into the system. The process of data mining involves the finding of links between various types of data and events, as well as the automated analysis and interpretation of data and events that come from a variety of sources as well as information from the individual who is utilizing it. There are a variety of applications for the skills and information gained through data mining, (Hentea, 2014).

Artificial neural networks are able to help categories, connect, and forecast future cyberattacks by learning from both historical data and current occurrences and then adapting as a consequence of what they have learned. For instance, in order to categories intelligence models, one may employ neural networks that can learn on their own without being seen (Hentea, 2014). You are able to evaluate qualitative factors and come to near conclusions using fuzzy logic, which is useful in situations when ideas are either incorrect or confusing. One model is used in the process of risk assessment. However, when diverse methods collaborate, they have the potential to assist build upon and emphasize the beneficial aspects of each model. This results in the person gaining information and intellect that may be beneficial to them. A possible way to use data mining, neural networks, and fuzzy expert systems together to prevent intrusion attempts is to use data mining and a neural network to find patterns of intelligence and classify them. Another option is to use data mining and fuzzy expert systems together to identify anomalies in data. This information may be submitted to a fuzzy expert system, which would then provide the individual with instructions depending on how well the infiltration attempts had been completed. Additionally, neural networks are able to recognize trends and provide predictions on potential cyberattacks. In addition, neural networks are able to figure out what's happening even when the information that they have isn't in its most complete form. The knowledge base contains a variety of different types of information pertaining to security, such as raw data and events, performance measurements, trends, rules, and choices. The process of information discovery, knowledge representation, and knowledge refinement are all vital components that make up a knowledge management system. One further thing to consider is how much it will cost to construct and maintain. The cost of the system must be prohibitive for

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

businesses; otherwise, they won't be able to invest in cutting-edge tools like data mining, artificial neural networks, fuzzy logic, and knowledge bases, which are all necessary for ensuring data safety and thwarting security breaches (Kaur & Rani, 2016). In spite of the fact that we have discussed a few different methods in which the system may operate, we have not provided a comprehensive list of needs. objective is to provide a blueprint for developing an information-processing system that is both clever and intuitive administration of the security system. Intelligent manufacturing systems that are comparable to these ones are discussed in (Dowd & McHenry, 1998).

4. ARCHITECTURE DESIGN

Language for describing a building's architecture an architectural description language is used to create a formal definition of the software architecture design model (ADL). ADL's formal model can be used to set up and check different properties automatically using a model checker. Using the Component and Connector view (C&C), includes syntax for defining the components, connectors, ports, and roles. A computational unit is represented by a component. Two or more components can communicate with each other by using a connector. Connectors can play multiple functions to demonstrate how various components interact. A component's ports can be used to connect to many roles. These design entities are defined using the process expression in Communicating Sequential Process (CSP).

4.1 Architecture in several new forms

In order to improve the development, deployment, and maintenance of systems, numerous technologies and practices have been developed. Because of this, the features of modern software systems are different than they were in the past. Large monolithic software systems are inherently difficult to maintain and improve. Breaking down a large complex system into smaller software components that can be placed together to serve various roles is the best approach to do this (Dragoni et al., n.d.). These components should be made, installed, and executed independently. As a result of this demand, an increasing number of people are becoming interested in learning about computer architecture. For the second time in this article, we'll explain how event-driven architecture builds loose linkages across dispersed software systems (Nadareishvili et al., n.d.). Decentralized data storage is safer and more dependable than employing a single point of failure or attack in a network since network components are dispersed.(Xu et al., 2016). As a result, blockchain technology enabled distributed storage. However, they are just a few of the many modern software systems have to offer. The way software systems are analyzed must be able to adapt to new technologies as they evolve.

There are two aspects to any intelligent system, according to (Meystel & Albus, 2002). There are four subsystems that make up the internal system, which can be split down into the following: As a result of this processing, the system's inputs are transformed into a consistent world state. Sensors are employed to keep tabs on the environment as

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

well as the internal workings of the intelligent system. A world model is a projection of how the world might look in the future. Knowledge of the world and a simulation module depict the world as it will be in the future are included. Decisions are made here about objectives, plans, and tasks via the behavior generating module.

Value judgement: This takes into account both the present and future conditions, and decides what to do next. Intelligent systems rely on the input and output provided by sensors and actuators, which are considered external components. It is a common feature of intelligent systems to have a sensory processing subsystem that uses data from sensors to create and update an internal model of the environment. A behavior-generating subsystem then determines how to accomplish the aim. The behavior generation subsystem controls actuators to assist the behavior achieve its goals in the context of the perceived world model. The outputs of intelligent systems are used to provide instructions to the target system. Cyberattacks can be detected and predicted with the help of sensor data, which is used to construct knowledge bases. Sensor data includes, for example, data on the following: performance, safety, and the current state. In addition to the device's CPU performance and memory usage, memory utilization, used disc space, and file usage are all factors that can be used to evaluate the performance of a computer system. These include the number of active connections, open connections, failed logins, number of transactions, new user requests, new software requests, user termination, response time, and the number of concurrent users.

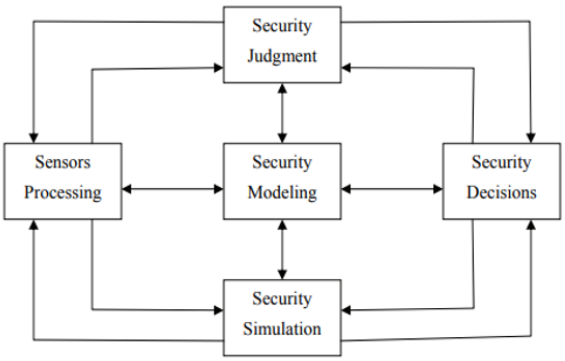

Figure: 1 Approach of self-containing adapted from (Hentea, 2014)

Based on a hybrid approach to applying intelligent models for decision-making, the system's architecture provides both strength and depth of understanding. Rather than relying just on a security expert to monitor and make decisions, this system aims to do more. People can also use this system to learn more on their own about potential dangers, regulations, procedures, and hazards. To be able to anticipate attacks, this system uses a flexible model that can handle a wide range of inputs and outputs. An event can be defined as any type of action, such as performing a virus scan or logging into a computer. A key element of design is creating an intelligent model for real-time event analysis and correlation. Intrusion detection systems, firewalls, anti-virus software

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

and spam filters are all better able to locate and stop security threats. As an example, neural and fuzzy models, should be able to alter, analyze, and classify events and data in a way that allows them to forecast attacks and provide user feedback. The fuzzy logic model is also helpful in risk management, an essential aspect of the life cycle of information security management (Hentea, 2014). Incorporating network monitoring, auditing, and physical and logical access control data into the models is also a good idea. Information security management responsibilities such as monitoring, detection, and threat identification could be made easier with these model-based tools. If they can help avoid attacks, they should also be able to provide relevant information on attacks that have already occurred, as well as forecasting future attacks. When a self-contained agent senses an object, it encodes, filters, and processes the data before sending it on to other components of the. Data is provided to components that organize, classify, integrate, and correlate data or create new information that is stored in the knowledge base, such as security modelling, security simulation, or behavior generators. Models of adaptive security event management are combined in the hybrid system. It makes use of artificial intelligence (AI) as well as statistical and more traditional procedural methodologies. For the most part, the rationale behind numerous models is that they can do different tasks using different measures and can compensate for each other. Artificial neural networks can be used to identify reconnaissance patterns, but the outputs or parameters can then be supplied to a fuzzy logic expert system that can interact with the patterns.

5. ANALYSIS OF RESULT

Information security management has been the subject of a wide range of studies. Information security and management, information security policy awareness and training, integration of technical and managerial activities for information security management, human aspects of information security management, and information security as a business issue. Information security and management Information security has been the subject of a great deal of technological innovation, but many organizations still struggle with it (Grant, Edgar, 2014) As a result, the problem should be approached from a managerial perspective, not just from a technical one.

5.1 Information security policy, awareness, and training

Additionally, there are research on the best practices for information security management, which are distinct from studies on general management. Policy development, policy awareness and training, and policy compliance are the most frequently discussed practices in the field of information security policy.

5.2 Integration of technological and managerial activities for information security

In order to effectively manage information security, it is also suggests integrating technical and management activities. In order to be a successful information systems manager, you must also have strong technical skills in the field.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

5.3 Information security and human resources management

Managing information security is all about people. In an organization, employees have a positive and negative impact. Employees, on the other hand, have the potential to inflict harm. A corporate organization's security is threatened by the fact that someone can steal information and disobey access regulations, which can have serious consequences (Vance et al., 2016). Information security will benefit greatly from personnel that adhere to security policies and are aware of security concerns, as well as those who have been taught.

5.4 As a business, information security is a major concern.

A company's share price and market position benefit from an effective approach to managing information security risk. Information security should be discussed in the same locations as other business issues that have a direct impact on a company's overall profitability (Chabinsky, 2014). Young & Windsor, 2010) Higher-level meetings should be used to discuss information security because it would be more linked with the company's overall strategy and procedures.

6. DESIGN ISSUES

Making the decision of which agents to include in the design is critical. A variety of agents can be created to aid in the administration of information security. A proposed system should have a decision-making agent and a control-making agent.

As a combination of its functions and smart abilities, an intelligent agent is commonly perceived. Some approaches use the term roles to describe the duties of agents. What the agents will perform can be deduced from combinations of functionalities. Most experts agree that an intelligent agent is situated, autonomous, reactive, proactive, and sociable despite much debate over what those terms mean and what attributes they entail. The field of autonomous agents has grown mostly because of artificial intelligence.

A hybrid architecture combining several types of intelligent agents is used in the suggested system due to the complexity of information security management activities. Information collection, sorting, and decision-making are all processes that can be automated by intelligent agents. Network administrators might benefit from their assistance as well. Agents should be designed to maximize their performance metric, which measures how well an agent behaves, according to Russell and Norvig (2003). Besides portability, stability, resilience, and security, other significant considerations include the agents and system's portability, stability, resilience, and security (Bradshaw et al., 2001). To keep the security process under control, the user interface should incorporate intelligent elements that aid in decision-making and action.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

Information security management needs should drive performance metrics, not arbitrary expectations about how an agent should behave. Additionally, you must choose what kind of feedback is provided for learning during the design phase. In order to figure out what kind of problem the agent must tackle, feedback is the most significant component. A distinction is often made between supervised and unsupervised learning in the context of machine learning. There are two ways to go about managing your organization's information security. Using both will give you the best results. Consider the mobility of the agents, which is their ability to move about the network at a given time.

The presentation of the data is an important aspect of the design. Information security management duties that can be accomplished with the knowledge that you already possess will also be considered in the design. Most learning begins with the agent having no prior knowledge of the subject matter. By observing how it interacts with and makes decisions in relation to its surroundings, the agent gains knowledge and experience. Smart behavior necessitates the continual pursuit of knowledge as a means of self-improvement.

It is possible to employ the spiral development method to develop the functions of each individual part. Depending on the demands of the organization, A model's implementation sequence will be determined by available resources and business requirements. When data and events are acquired from various sources, data mining helps to automate the analysis and interpretation of the data. A user can get feedback and information from this system as well. The following are some real-world applications of data mining and knowledge discovery (Adebukola Ibrahim et al., 2005) The use of artificial neural networks, which can learn from both the past and the present, aids in the classification, linking together, and forecasting of cyber threats in the future. Reconnaissance patterns can be sorted using unsupervised neural networks, Intelligent Information Security Management System Allows for qualitative variables and approximation reasoning when the premises are ambiguous. One model is used to do the risk assessment.

It's possible to bring out the best features of each model by combining diverse approaches. As a result, new information and insights are generated, which in turn aid human decision-making. Recon patterns can be uncovered by using data mining techniques, neural networks, and fuzzy expert systems in conjunction with each other in the fight against infiltration attempts. When an incursion is detected, this information can be given to a fuzzy expert system, which can subsequently advise the user what to do. The ability to recognize trends and anticipate cyberattacks is another benefit of neural networks. Even if some of the input is unclear or ambiguous, neural networks can nevertheless figure out what's going on. Raw data and events, performance metrics, patterns, policies, and judgments are all part of the knowledge base. Knowledge refinement, knowledge representation, and knowledge discovery are all necessary components of a knowledge management system. Development and maintenance costs are also critical. In order for organizations to leverage modern security

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

technologies like data mining, AI, fuzzy logic, and knowledge bases, the system should be economical enough (Kaur & Rani, 2016). While some of the system's characteristics were discussed, not all of the prerequisites were addressed. (Dowd & McHenry, 1998).

7. CONCLUSION

Recognizing, filtering, and linking events and data from diverse sensors and sources needs cutting-edge real-time techniques that combine modelling, sensor analysis, and intelligent agents with standard procedural and statistical methods. These technologies open the path for automated reactions to concerns and effective recommendations for preventing future attacks. We present a unique method for constructing an intelligent data protection monitoring system. The proposed architecture is based on the disciplines of information security management, network communications, computing, artificial intelligence, modern control theory, statistics, social sciences, organizational theory and behavior, management science, business strategies, risk analysis, and economics. Cyberthreat growth and complexity cannot be halted by a single remedy. Clearly, a mix of paradigms is necessary to accomplish the information security management goals of a 21st-century organization. In many respects, the fields of cyber security and intelligent agent technologies are closely intertwined. It builds upon previous research in artificial intelligence and related fields. Similar systems or prototypes have not yet been identified. Although prototypes of features and components are starting to appear, more refining and assembly are necessary. Since information security knowledge is always growing, the system must be sufficiently flexible to include it. Future efforts should strive to provide a proof-of-concept that demonstrates how each module contributes to the overall and assists in security management.

Future work

Using quantitative surveys and qualitative case studies to validate the research's results might also help us understand the difficulties this article raises. Security concerns in corporate design, information infrastructure, and cloud computing are also highlighted from a managerial perspective in this research.

Author Contributions

All authors have equal contribution.

Conflict of Interest

There is no conflict of interest between all the authors

Funding

This research received no external funding.

Reference

1. Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, R. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). Journal of Sensors, 2022..

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

2. Adebukola Ibrahim, S., Folorunso, O., & Bamisele Ajayi, O. (2005). Knowledge Discovery of Closed Frequent Calling Patterns in a Telecommunication Database. Proceedings of the 2005 InSITE Conference. https://doi.org/10.28945/2938
3. Bhatti, R., Bertino, E., Ghafoor, A., & Joshi, J. B. D. (2004). XML-based specification for web services document security. Computer, 37(4), 41–49. https://doi.org/10.1109/MC.2004.1297300
4. Bradshaw, J. M., Suri, N., Breedy, M., Cañas, A., Davis, R., Ford, K., Hoffman, R., Jeffers, R., Kulkarni, S., Lott, J., Reichherzer, T., & Uszok, A. (2001). Terraforming cyberspace Terraforming Cyberspace. August. https://doi.org/10.1109/2.933503
5. By, E. (n.d.). Computer Science and Security.
6. Chang, R. K. C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Communications Magazine, 40(10), 42–51. https://doi.org/10.1109/MCOM.2002.1039856
7. Dowd, P. W., & McHenry, J. T. (1998). Network security: It's time to take it seriously. Computer, 31(9), 24–28. https://doi.org/10.1109/2.708446
8. Dragoni, N., Giallorenzo, S., Lafuente, A. L., & Mazzara, M. (n.d.). Microservices : yesterday , today , and tomorrow. 1–17.
9. Grant, Edgar. (n.d.).
10. Hentea, M. (2014). Intelligent System for Information Security Management : Architecture and Intelligent System for Information Security Management : Architecture and Design Issues Cyber Security Overview. October. https://doi.org/10.28945/930
11. Hosny, A., Parmar, C., Coroller, T. P., Grossmann, P., Zeleznik, R., Kumar, A., Bussink, J., Gillies, R. J., Mak, R. H., & Aerts, H. J. W. L. (2018). Deep learning for lung cancer prognostication: A retrospective multi-cohort radiomics study. PLoS Medicine, 15(11), 1–25. https://doi.org/10.1371/journal.pmed.1002711
12. Kaur, G., & Rani, P. (2016). II . EXPERT SYSTEM IN IS AUDIT III . ISSUES OF EXPERT SYSTEM. 7(6), 163–165.
13. Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in e-learning systems. Journal of Supercomputing, 78(3), 3325–3354. https://doi.org/10.1007/s11227-021-03981-4
14. Meystel, A., & Albus, J. (2002). Intelligent Systems : Architecture, Design, and Control / A.M. Meystel, J.S. Albus.
15. Nadareishvili, I., Mitra, R., Mclarty, M., & Amundsen, M. (n.d.). Microservice Architecture.
16. Norvig, P. (n.d.). Artificial Intelligence.
17. Sametinger, J. (2013). Software security. Proceedings of the International Symposium and Workshop on Engineering of Computer Based Systems, 216. https://doi.org/10.1109/ECBS.2013.24
18. Seifert, D., & Rez, H. (2016). A security analysis of cyber-physical systems architecture for healthcare. Computers, 5(4). https://doi.org/10.3390/computers5040027
19. Sun, H., & Bai, S. (2022). Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology. Computational Intelligence and Neuroscience, 2022, 1–16. https://doi.org/10.1155/2022/7138515

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/8CKV5

20. Taibi, D., Lenarduzzi, V., & Pahl, C. (2018). Architectural patterns for microservices: A systematic mapping study. CLOSER 2018 - Proceedings of the 8th International Conference on Cloud Computing and Services Science, 2018-Janua, 221–232. https://doi.org/10.5220/0006798302210232

21. Tang, X., & Ding, C. (2021). Information Security Terminal Architecture of Power Transportation Mobile Internet of Things Based on Big Data Analysis. Wireless Communications and Mobile Computing, 2021. https://doi.org/10.1155/2021/5544716

22. Vance, A., Lowry, P. B., Eggett, D., Vance, A., Lowry, P. B., Using, D. E., Vance, A., Lowry, P. B., & Eggett, D. (2016). Using Accountability to Reduce Access Policy Violations in Information Systems Using Accountability to Reduce Access Policy Violations in Information Systems. 1222(March). https://doi.org/10.2753/MIS0742-1222290410

23. Wang, F.-Y. (2005). Agent-Based Control for Networked Traffic Management Systems From control algorithms to control agents.

24. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016, 182–191. https://doi.org/10.1109/WICSA.2016.21

25. Yu, W. D., & Le, K. (2012). Towards a secure software development lifecycle with SQUARE+R. Proceedings - International Computer Software and Applications Conference, 565–570. https://doi.org/10.1109/COMPSACW.2012.104

26. Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. Applied Sciences, 12(21), 10794.

27. M. Akram, M. Waseem Iqbal, S. Ashraf Ali, M. Usman Ashraf, K. Alsubhi et al., "Triple key security algorithm against single key attack on multiple rounds," Computers, Materials & Continua, vol. 72, no.3, pp. 6061–6077, 2022.