Migration Letters

Volume: 19, No: S5 (2022), pp. 1156-1171

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Assessing The Information Security In IT Industry: A Conceptual Framework For Successful Implementation Of Information Security Management System

Gulnaz Niazi[1] , Dr. V.K Panchal[2] , Prof. Mansaf Alam[3]

ABSTRACT

The goal of the security management information system is to consider both the intent behind content disclosure and the implications of that use within the company. The precise division of information management affects the enterprise's operati[1]onal activities and leads to group decision-making on information protection against outside unlawful use or data transfer to a rival organization. After reviewing earlier research on 'Information Security Management System' as an outcome variable in the Indian IT industry, this study will discuss 'Firewall security', 'Logic based security', 'Problem of deleted data recovery' and 'success of security management information system'. The literature study also includes a presentation of the independent factor, 'Information Security awareness (ISA)' that have been chosen to influence 'Firewall security', 'Logic based security', as well as 'Problem of deleted data recovery' in IT industry in India. Finally, a conceptual model has been proposed assessing the relationship among 'Information Security awareness (ISA)', Firewall security, Logic based security, Problem of deleted data recovery and success of security management information system

***Key words**: Information Security awareness, Firewall security, Logic based security.*

1. INTRODUCTION

In the era of globalization, protection of information is critical in order to ensure business continuity S. E. Chang (2006). Addressing security breaches became a challenge for organizations. Information Security (IS) is a concept that is related to protecting information in order to preserve the value it has for organisations and individuals Information's confidentiality, integrity, availability, authenticity, accountability, and reliability are ensured through IS. Organisations which are lacking in IS will usually prone to a large number of security breaches and incidents W. Al-Salihy (2003) recognising this, many organisations have put in place substantial efforts in managing and handling the security of their information. They have implemented Information Security Management (ISM) initiatives by reviewing IS processes, policies, procedures, controls and organisational structures. ISM is a comprehensive approach that involves the implementation of activities and controls to protect organisation's information assets from any intrusion. In spite of the efforts, organisations are still exposed to information security threats, incidents, vulnerabilities and risks M.A.M (2011) One of the contributing reasons is the ineffective ISM current practices. Organisations often emphasise on the technical

[1] Research Scholar, Department of Computer Science, Al-Falah University, Dhauj, Fridabad, Haryana, India
[2] PhD Supervisor, Department of Computer Science Al-Falah University, Dhauj, Faridabad, Haryana, India
[3] PhD Co- Supervisor, Department of Computer Science Faculty of Sciences, Jamia Millia Islamia, New Delhi, India

aspects without appropriate considerations on the non-technical aspects when implementing ISM Shojaie and H. Federrath (2015).They normally perpetrate into the initiatives without knowing the key factors that affecting its success N. Maarop et al (2015). Based on the above facts, there is a need to identify the key factors that contribute to the success of ISM. This paper addresses this issue by identifying and collating the key factors from theoretical and empirical perspectives. The identified factors will be incorporated in the form of a proposed conceptual framework for this study to strengthen the success of information security management system.

2. OBJECTIVE OF THE STUDY

Study of Security Management Information System in relation to Information Technology

- Proposal of conceptual model assessing the relationship of Firewall concepts, logic and findings and Problem of deleted data and their impact on Security Management Information Systems

3. LITERATURE REVIEW

3.1Information Security (IS)

Information security is concerned with the identification of an organization’s electronic information assets and the development and implementation of tools, techniques, policies, standards, procedures and guidelines to ensure the confidentiality, integrity and availability of these assets.

Information security means protecting information and information systems against unauthorized activities such as unauthorized access, use, disclosure, and reading, copying recording, destruction, revision and manipulation (F, Bjorck. 2001; Bokhari, S. and Manzoor, S. 2022). In fact, information security relates to confidentiality, integrity and availability of data, regardless of information form including electronic, print of them forms. Computer security focuses on ensuring being availability and proper functioning of a computer system without any concern about information that is saved or processed by the computer system, government, military agencies, corporation, financial institutions, hospital and private occupations collect large amount of confidential information about employees customer, products, researches and financial condition. Most of this information is already on electronic computers collected, processed and stored and transferred in the network to other computers. If conferential information about customers and/or financial issues or new institute financial product is taken by arrival, this information leakage might lead financial loss to a business, legal pursuit and /or even bankruptcy. Protecting confidential information is a business need and in many cases a moral and legal need as well. For people, information security has a significant effect on privacy (A. Rathmell. 2001).

Infact information security consists securing information and minimizing unauthorized access to it and also the science of study of the methods to protect data in computer and communicative system against unauthorized change. Information security is the protecting of information for confidentiality, integrity and accessibility (P. Williams. (2001; Kamariotou, M.; Kitsios, F. 2023). Additionally, other features such as authenticity, responsiveness, credibility (validity), irrefutability, information reliability can also include this sort of protection.

3.2Security Management Information Systems (SMIS)

Determining success factors in SMIS is essential as it provides a useful indicator of essential security management practices required in a business. This indication will provide a general idea to the companies to adopt appropriate SMIS for their business. Consequently from this determination, company could invest on proper SMIS practice which is achievable with the business objectives. Thus, only required resources are used and utilized without waste. Besides giving information to the organization on how to stay safe and secure in the business, SMIS success factor also demonstrates the successful elements business must anticipate preventing IS failure. Today, almost all businesses rely particularly in IS where security management is inseparable feature to ensure business stays safe and secure.

Scholars like Ein-Dor and Segev (1978) have asserted in their study of the management of IS that in an organizational context, organizational factors consisting of organizational size, business type and management support are the main determinants of MIS success. The organizational factors are again used in Kankanhalli et al. (2003)'s study of information system security effectiveness. She found that similar factors are applied in determining IS security effectiveness. Because this study looks at e-commerce as the organizational context in the study of information systems security management success factors, similar organizational factor is also considered and is accepted as part of attributes to be analyzed.

Security Management Information Systems (SMIS) connotes the holistic security management in a business. SMIS looks at people, process and technology issues, of a business environment (Wu, W., Shi, K., Wu, C. H., & Liu, J. 2021). It is necessary for a business to look into people, process and technology perspectives (James, 1996). This is because information systems are not just about the technology, but the people- creator and users, and process-involving internal and external environment of related business. It is most appropriate and logical to use the theoretical model developed, because it supports the bigger picture of SMIS concept. The challenging part is to accommodate the attributes in each theory to suit the TOE umbrella, which is discussed separately from this article. As the Internet is exempted from controls, appropriate SMIS is highly needed toensure safe and secure transactions between users and the business entity, thus providing trustworthy information systems. Security management signifies the process of implementing and exercising security measures appropriate towards a business with the objective to mitigate risk and threats. Security management must also decide on business in attempts to withdraw any security measures due to change of business objective or upgrade of the information systems. The same security management exercise and meaning is reflected in many security standards and best practices including ISO27002, GIASP and Standard of Good Practices. Many scholars also discuss similar meaning of security management in their studies (Kritzinger and Smith, 2008; Sanchez et al., 2006; Siponen and Willison, 2008; von Solms, 2006; von Solms and von Solms, 2004; Zuccato, 2007; Bokhari, S. and Manzoor, S. 2022) Thus, it is justly to say that security management involves businesses to implement, exercise and monitor appropriate security measure to protect and safeguard business assets in the business information systems.

Reflecting on the security management meaning, there are so much to be done to qualify company to be a wise security management user. There is no rule of thumb but there are many considerations to it such as highlighted by von Solms and von Solms (2004; Tewamba, et.al. (2019).

3.3 Information Security Awareness

Hänsch and Benenson (2014) discuss three different meanings of information security awareness from how most researchers have viewed it. The researchers have tried to define information security awareness as a concept and came to the conclusion of these three meanings in which you can have a viewpoint from.

Security awareness as perception contains the views of researchers which concludes that information security awareness means that users should know that threats, dangers and risks exists (Hänsch&Benenson, 2014). "If an individual perceive the threat, that individual can be described as having awareness of a threat." (Johnston &Warkentin 2010, cited in Hänsch&Benenson 2014, p. 326). This statement defines the meaning of security awareness as perception. End users responds individually to different security threats and the response is decided by which kind of perception the individual have of that specific threat. Security awareness as perception also relates to the degree an end user thinks something is secure or not (Huang, Rau, &Salvendy, 2010).

Security awareness as protection contains the views of researchers which demands that the users should be aware about which threats, dangers, and risks exists, and the users should also be aware of which kind of measures they can apply to protect themselves. This meaning of security awareness is about users' attentions on security and how well they recognize IT security problems and concerns, and how they should respond (Hänsch&Benenson, 2014).

Security awareness as behaviour contains the views of researchers that concludes that the main reasons of information security awareness is to reduce security hazards effectively. This is reached when users know which kind of security measures they can use to protect themselves and how to deploy and maintain software applications. This meaning of security awareness focuses on how users act and think regarding information security, and the degree of which you can transfer knowledge of different factors in information security that may influence the way a user acts or behave (Hänsch&Benenson 2014).

Information security awareness as a research field has been given increasingly important focus over the years, and has become a well-researched area. The focus of researches lies in the view of information security awareness of organizations and their end users, and how they should promote, protect and work with security awareness (Furnell, Bryant &Phippen, 2007; Arcy, Hovav&Galletta, 2009; Kritzinger&Solms, 2010). This has then led to that the academia, government and the industry has developed and implemented numerous information security awareness programmes (Kritzinger&Solms, 2010). According to Talib, Clarke &Furnell, (2012) researches focus has also been on how and what to educate end users in, at organizations.

Furthermore, in order to ensure that education leads to practice, researchers has identified that it is important to measure how effective the organization's security awareness training really is.

3.4 Firewall

Firewall is a security defense tool applied in the field of computer network security. It's used between the intranet and the extranet. The former is recognized as a secure network. The latter is identified asa relatively less secure network. The firewall consists of software and hardware. Connectivity between the intranet and the extranet must and can only pass through the firewall. Firewall is the basic service means to guarantee network information security. It's very protective. At the same time, the information flow in and out of the network can be released and intercepted by receiving the security policy control (permission, rejection, monitoring) and so on. The firewall is an analyzer. Be able to analyze the information flow through. And a separator, you can filter the analyzed information flow. It's also a limiter, restricting the flow of information that is screened as unsafe. Denying access to the intranet, authorize secure information flow into the intranet. Authorize secure information flow into the intranet. Therefore, it can effectively protect network security. Ensure the security of the intranet. Firewalls used to be partitions in buildings to prevent fire from spreading. Here is extended to protect the internal network security of a protective wall Tang (2018).

3.4.1 Studies on Firewall Security

Wool performed two quantitative studies A. Wool, (2004) of firewall ruleset configuration errors in real, deployed firewalls. Both of these studies suggest that firewalls, in general, are poorly configured and that the number of configuration errors is positively correlated with the number of rules in the ruleset. Wool's studies and our study are tangentially related, but while Wool studied the phenomena of configuration errors in great detail, our study discusses it with broader strokes as part of a bigger picture. Furthermore, Wool defines a firewall configuration error as being any configuration of a set of configurations that he considers to be insecure in some way. Even though the research is probably the best of its kind, the studies, as well as Wool's set of configuration errors, are rather old. This study aims to address both the definition of configuration errors and the relevance of previous research.

Kamara et al. (2003) propose a methodology for analyzing vulnerabilities in firewalls. Twenty known firewall vulnerabilities are analyzed and categorized according to the suggested methodology.

Alsaleh et al. (2013) present a set of quantitative metrics for measuring the security level of an enterprise firewall based on its ruleset configuration. The metric can be used to compare the security of different firewalls against each other. While the metric is useful for many purposes and certainly would be interesting to apply to data such as Wool's, we cannot make use of it given our choice of research methods. This study instead explores an alternative approach to estimating firewall security.

Firewall testing has different goals, including determining if the firewall is a correct implementation of the firewall security policy, how well the firewall resists particular types of attacks, if leakage occurs in the security perimeter created by a firewall, if the logging capability is adequate, if the firewall has the ability to send alarms, and if the firewall can hide information and addresses from the internal network it protects E. Schultz (1996). The basic design of a firewall and sample firewall algorithms are discussed in Schuba formalizes firewalls using hierarchical colored Petri nets. Bellovin S. Ioannidis et al (2000) recently proposed a distributed approach to Internet firewalls. In this approach, personal firewalls are installed at the hosts themselves. The advantages of this distributed approach include detection of attacks within the internal network, detection of more application level attacks, and speeding up firewall functions.

In Haeni (1997) describes a methodology to perform firewall penetration testing. The testing steps include indirect information collection, direct information collection, attacks from outside, and attacks from inside. Attack approaches are based on the type of firewall. For packet filtering firewalls, the attacks include blind IP spoofing, non-blind IP spoofing, source porting and source routing. For application level firewalls, the attacks are on bad security policy, poorly implemented policies, SOCKs incorrectly configured, brute force attacks, and enabled services/ports.

Another firewall testing methodology is presented in Giovanni (2000). The field testing is currently performed using simple checklists of vulnerabilities without taking into account the particular topology and configuration of the firewall target operational environment. A firewall testing methodology is proposed, based on a formal model of networks that allows the test engineer to model the network environment of the firewall system; to prove formally that the topology of the network verifies the sufficient conditions for protection against attacks; and to build test cases to verify that protections are actually in place.

In Lyu and Lau, (2000), firewall security and performance relationships are explored. Experiments are conducted to classify firewall security into seven different levels and to quantify their performance effects. These firewall security levels are formulated, designed, implemented and tested under an experimental environment in which all tests are evaluated and compared. Based on the test results, the effects of the various firewall security levels on system performance with respect to transaction time and latency are measured and analyzed. It is interesting to note that the intuitive belief that more security would result in degraded performance does not always hold.

In addition, the Internet engineering task force (IETF) has examined Internet firewalls. RFC 2647 D. Newman (1999) extends the terminology used for benchmarking routers and switches with definitions specific to firewalls. Forwarding rate and connection-oriented measurements are the primary metrics used in the RFC. RFC 2979 N. Freed (2000) defines behavioral characteristics and interoperability requirements for Internet firewalls. The RFC observes, that firewall behavior is often either unspecified or under-specified, and this lack of specificity often causes problems in practice. Requirements specification makes the behavior of firewalls more consistent across implementations and inline with accepted protocol practices.

H1: Information Security awareness (ISA) can have a favorable impact on firewall to be more consistent across implementations.

H2: The specified firewall behavior can have a favorable impact on the success of security management information system.

3.5Logic-Based Security

When two entities communicate to obtain a certain service(s), they must ensure secure end-to-end communication. Systems do not provide efficient services without applying proper security mechanism due to the existence of different types of attackers. Security can be defined through a set of requirements that must be achieved by the communicating parties to communicate securely and protect services from attackers.

Because of the importance of security for end-to-end communication, many secure protocols have been proposed as will be discussed later in the paper. Some of these protocols had taken prevention measures to stop attackers while others had taken the detection approaches. A way to analyze these protocols is required to check if these protocols are secure as their designers claim and to know which security requirements these protocols achieve. In this paper, we propose a logic-based security architecture (LBSA) which is an easy, fast, and reliable way to specify and analyze secure protocols.

Some security requirements, as defined by several standards such as ITU-T Recommendations X.800 and X.805 (ITU-T 1991, ITU-T 2003), must be achieved to declare that a protocol is secure. Using LBSA, a protocol can be tested to check which security requirements it achieves. Several efforts have been done to utilize logic in such test (A. D. Rubin et.al 1994 - A. D. Rubin 1997), Utilizing LBSA, protocols can be tested to check if they achieve the security requirements specified by their designers. This checking can be performed by analyzing the protocol and applying appropriate actions and rules. If the rules are applied successfully we conclude that their claim is true, otherwise it is false.

3.5.1 Studies on Logic Based Information Security System

The importance of security in providing successful services in any distributed system raises the necessity of having formal way to analyze security protocols. Previous effort in using logic for analyzing security is Rubin logic (A. D. Rubin et. al. 1994, A. D. Rubin 1997).

Rubin logic is an approach that specifies and analyzes non-monotonic cryptographic protocols. It is one of the first approaches to allow reasoning about non-monotonic protocols (A. D. Rubin et. al. 1994). In non-monotonic protocols, beliefs are changed during protocol execution time. An example of non-monotonicity is the belief that a key must be changed when a node becomes compromised. To achieve the protocol specification and analysis, Rubin logic defines global and local sets, actions and inference rules.

Rubin and Honeyman (A. D. Rubin et. al. 1994) focused on authentication protocols. They took KHAT protocol (A. D. Rubin et.al. 1993) as an example to discover its laws. KHAT protocol was built to solve the problem of long running jobs in an authenticated environment where a trusted server issues tickets with limited lifetimes for services. The authors gave special attention to ensure the freshness of data using fresh nonce. The main problem they attempted to solve is that principal B cannot achieve the belief that the session key with principal A is fresh. Finally, the authors defined most of global and local sets that are use later in the literature.

Rubin (A. D. Rubin 1997) extended the work presented in (A. D. Rubin et. al. 1994) by adding one set. Rubin (A. D. Rubin 1997) aimed to make sure that keys are observed by their intended parties and data items are fresh, especially the public keys. Rubin (A. D. Rubin 1997) made link between certificates and requests which reveals weakness in Needham and Schroeder public key protocol (R. M. Needham 1978).

Xu and Xie presented in a series of papers (Y. Xu et. al. 2008–Y. Xu et. al. 2008) the utilization of Rubin logic in analyzing the security for specific protocols.

In (Y. Xu et. al. 2008), Xu and Xie extended the work presented in (A. D. Rubin 1997) to analyze nonrepudiation in routing protocols proposed for wireless mobile ad hoc networks (MANET). This work took ARAN (11) routing protocol to test nonrepudiation.

Xu and Xie (Y. Xu et. al. 2008) use the work presented in (Y. Xu et. al. 2008) to analyze electronic commerce protocols and in (Y. Xu et. al. 2008) they have chosen Zhou-Gollmann (J. Zhou 1996) protocol which is a simple and effective nonrepudiation protocol to illustrate how an electronic commerce protocol is analyzed using the extended Rubin logic.

Two examples of Rubin logic’s applications are given by Xu and Xie in (Y. Xu et. al. 2008). First example is the Andrew secure RPC (M. Satyanarayanan 1989) protocol using symmetric keys. The second one is X.509 (ITU-T 2008) authentication protocol using asymmetric keys.

As can be illustrated from the above-related work, all attempts to utilize Rubin logic have either focused on a specific requirement or a specific protocol. This paper proposes a logic-based security architecture (LBSA) that presents a formal way to analyze any security requirement in any system providing multihop communication. All sets, actions, and rules presented in previous efforts are considered and generalized; new ones are added to complete the architecture. After that, we illustrate how LBSA will be used to test security requirements and issues in different security enforcers and protocols.

Fuzzy logic has been used in a wide variety of systems such as the automatic focus of digital cameras (Yang WR, et.al. 2002), control and optimization of industrial processes and systems (Lee CC. 1990), improving the efficiency of fuel-running engines (Lee S, et.al. 2004), environmental improvement (d S C Boclin A 2006), expert systems (Yager RR,et.al. 2012), robotics (Antonelli G,2007), vehicles and autonomous driving (Wang X et.al. 2015), computer technology (Trillas E, et.al. 2015), Fuzzy databases (Galindo J.2008), artificial intelligence, control systems for air conditioners, family appliances (Kolokotsa D.2011, Ciabattoni L, et.al. 2013), wireless sensor networks (Kolokotsa D.2011–Manjunatha P,et.al. 2008), and cellular automata (Jaberi S, et.al. 2017–Tsompanas MAI et.al. 2018).

Concerning formal verification of IoT systems, the authors in survey (Souri A, et.al. 2019) present various works focused on verifying security properties (Bae WS 2019–Aktas MS et.al. 2019).

Input data in IoT systems is usually collected from heterogeneous sensor devices that need more interoperability since data values are based on proprietary formats. Similarly, IoT systems can accumulate poor-quality data since events such as offset data, missing data, wrong time stamps, and wrong attribute values can occur. Verifying the consistency of collected data has traditionally used machine learning and point-based calibration algorithms. For instance, authors in (Jiang H et.al. 2021) proposed a data consistency method based on neural networks to reduce data errors by approximately 4%. However, this approach cannot interact in real-time with end users since it verifies consistency before the system starts.

Logical data inconsistencies have also been studied in the description logic (DLs) setting comprising a family of knowledge representation languages (Baader F et.al. 2004). The balance between computational complexity and the expressiveness of DLs has allowed efficient reasoning tools to be constructed. These tools have enabled the application of DLs in several domains successfully (Baader F et.al 2003). Notably, the Web Ontology Language (OWL), a standard for Web Semantics technologies, is based on DLs (Baader F, et.al. 2005). Fuzzy extensions of DLs have also been developed (Bobillo F, 2008). These extensions have found application in human activity modeling for ambient intelligence systems (Rodriguez ND,et.al. 2014), diabetes diagnosis systems (El-Sappagh S, et.al. 2015), and database systems (Morente-

Molinera JA et.al 2015), to mention a few. Authors in (Reda R,2018) proposed a consistency data representation for IoT healthcare systems, transforming health data obtained from heterogeneous IoT devices into a semantic data model that supports logical reasoning using OWL. Even when the authors used a logic reasoned, they only focused on creating a unified static data model in which new rules cannot be introduced on running time. In (Bamgboye O,2019), the authors proposed a reasoning framework to guarantee the consistency of the data stream produced by physical sensors in smart spaces. However, this framework does not interact with end users.

H3: Information Security awareness (ISA) can have a favorable impact on logic based security implementations

H4: The logic based security implementations can have a favorable impact on the success of security management information system.

3.6Problem of Deleted Data

Data are valuable nowadays and if are lost, may cause a negative impact on the organization financial costs and time to regain it, so protecting important data, are required efficient countermeasures. During this decade cloud computing has become a new technological option to provide services and cloud providers are gaining even more popularity due to the increasing amount of data. The expanded usage of cloud computing services increment the need of more storage, backup and recovery.

Backup is defined as a duplication of any data, file, application and operating system that can be used in case of a data loss or restoration, while recovery is the set of techniques used to collect data from any backup server, when data are previously lost from the server or invalid to use.

Disasters effect both the client and the cloud side, hence it is crucial to have a disaster recovery plan. As it is mentioned by (A. Arul Mary, K. Chitra (2019) when "disaster happens in customer side means backup will be stored in the cloud, but disaster happens in the cloud means data will be lost. So, disaster recovery process is urgently needed. But quality and security are the key issues in the information recovery process" Tyagi et al (2019).

Even though there are still many technological gaps, for many organizations, cloud computing is a flexible, cost- effectively, reliable and scalable solution to provide a safe data backup and recovery. The organizations must identify the major probable failures that can cause a disaster for them, and then prepare a disaster recovery plan (DRP) and data backup.

DRP is a document that prepares and helps organizations to protect and prevent damages from a disaster. This plan usually addresses any type of disaster, however, it is customized based on the needs of the organization where the most important elements included are related to identifying and assessing disaster risks and determine the critical applications and resources.

As we know, most of the data and applications are found and stored digitally. The risk of data loss is relatively high regardless of the cloud environment, provider, services, or architecture. No matter if the data are stored in a Public or Private Cloud, data can still be corrupted at any stage. Therefore, to maintain the data safety, control, and accessibility it is required a strategy, including a backup and disaster recovery plan.

3.6.1 DATA RECOVERY

Data recovery is the process in which corrupted, lost or damaged data is recovered or retrieved from storage devices. This method is used when the data is inaccessible by normal means i.e. either the data inside is corrupted or completely formatted, or when the storage device is damaged and the method is used on devices like SD Cards, Hard Disks (Internal and External), SSD Devices, CDs and DVDs, and any other storage device D Drives (2017)

3.6.2 Studies on Recovery of Deleted Data

In correspondence with Bardis et al (2017)concludes that data recovery services must ensure high data reliability and flexibility through an effective and practical data recovery plan that sustain growth for any organization. According to the authors, the most critical issues relevant to data recovery in cloud computing focus on cloud data storage, cost, security, lack of latency and redundancy. Different strategies attempt to manage the data recovery process. They also highlighted that natural and manmade disasters can result in costly service interruptions.

In the literature survey of Faria et al (2019) they found many techniques that have their unique ways to create backup and recovery. The experimental results, done by Zhong& Xiang (2012), shows that many organizations and companies have utilized disaster recovery solutions to minimize the downtime and data loss incurred when catastrophes take place. All these approaches aim to provide the best performance.

Organizations are subjected to hazards that might interrupt options. From the point of Service Provider, client satisfaction is among the major objective, while from the business aspect, recovery means being able to perform business functions without affecting continuity. Data recovery services should assist business continuity, enabling applications to quickly come back online after a disaster happens (Alshammari et al. 2017).

A paper by (Suguna et.al.2014) states that organizations generate a lot of helpful information electronically in the modern world. This data needs to be saved in a secure place. Data recovery and backup issues are becoming very popular in networks nowadays. Due to the increase in data creation, the value of its safety is increasing every day. To meet goal recovery objectives in the modern world, business organizations require a proper backup plan at an affordable cost. Organizations must assess the likelihood of disasters and their potential implications. Supporting data is necessary for resistance against significant failures; in many cases, keeping backup information is regulated by law. The main objective of this paper is to show different cloud solutions that can help people and organizations manage their data. The comments in this article can be used to weigh the various options. To generate specifications, the application should first be investigated in terms of computational requirements and RTO. It is necessary to collect sufficient data to create construction models that will eventually allow the problem to be set up as a mathematical optimization. It is possible to create a model that links RTO and cost. According to some studies, the relationship between RTO and cost is non-linear.

Another paper written by (Singhet. al. 2012) says that nowadays, data acts as fuel for different organizations. There is a lot of important information created by companies every day, so it is essential to save this information in a secure place. Therefore, we have different cloud platforms to do this job for us. Cloud platforms provide various organizations and infrastructure where they can store and play with their data. This makes the cloud a safe place for organizations. Due to the creation of a lot of data, the demand for an efficient technique is increasing to secure and manage company data. Many different strategies have been offered so far to attain this goal. We look at some current strategies in the form of disaster recovery techniques and online data backup in this review paper. This review article aims to compile a list of the most effective data backup and recovery solutions utilized in the cloud computing area. Of all the solutions examined in this research, the PCS is the most trustworthy solution because it protects each resource’s privacy and costs very low.

The study by (Baginda et al. 2018) claims that the application’s accessibility is incomparable. So, the application should be available twenty-four hours a day, seven days a week. The response time should be a blink of an eye because even for a single minute if the application is not investigated, this can cost the company’s reputation and create substantial business problems. Now big organizations require cloud service providers to duplicate their infrastructure to make service available every time. Also, cloud providers are now providing data recovery services to help businesses recover their systems in the event of a disaster and maintain business stability. Many companies are still unsure which service will best fit their needs. RPO and RTO are two critical indicators for efficient data recovery. This paper focuses on the creation and implementation of two clouds and compares two parameters between them. In prior studies, prices, infrastructure, management, location, and other variables were used to compare data recovery providers. There is no way to measure disaster recovery between cloud service providers. Therefore, an implementation strategy is introduced in this research.

Security is the most important factor to consider when choosing a cloud storage provider because cloud storage is the location for data, and three aspects of data security must be met. The cloud can be used as storage. The cloud should be checked and appropriately studied before trusting it completely. As time passes, innovations keep taking place. Now, numerous cloud and storage options are available for managing your profile and data online. Clouds ensure that your data is safe and secure over the internet." Companies that provide high-end encrypted and safe storage, Google Drive and Dropbox, estimate that 15% of commercial Cloud users have experienced hacking.(Agus et al 2019) "Speaking about its security and privacy policies, Google states, "Our committed security team includes some of the world's best specialists in information security, application security, encryption, and network security. They also mentioned that the workers are well trained for the type of work they do. To give its customers the best experience possible, Google Cloud has cultivated a tight connection with the security research community. Google Cloud's team engages in ongoing research in an effort to enhance its facilities over time. Our committed privacy team provides support for internal privacy efforts aimed at enhancing privacy infrastructure, internal tools, products, and crucial procedures. (Saleem et al 2020).

One major concern is the possibility of overwriting a file on the cloud and forgetting to erase it. Data assurance, often known as cloud security, guarantees that your file is deleted entirely from the cloud. Each backup version was usually generated for the preceding version. If a file exists in more than one version, it is typical to store only one copy of it. Before entrusting the cloud with their files and data, an individual should properly investigate the cloud and its policies. Sarwar et al (2019) Hussain (2021) One of the most important problems in cloud computing environments is data backup and recovery, and there is a constant need for workable methods of doing so. In order to guarantee availability and dependability in the cloud, fault tolerance is a serious concern. When the server cannot provide the users with the data or when the data has been lost as a result of one of various failure scenarios, the data recovery procedures are employed to recover the data from the backup server. Examples of cloud computing problems (hardware failure, application failure, etc.), their fixes (proactively tolerant of faults, dynamic clustering, etc.), and administrative tools and techniques (seeded block algorithm, parity cloud, etc.) were covered in this study. L. Saleh (2020).

Cloud computing appeals to information technology specialists since it combines multiple developing technologies. In addition, a multi-server solution based on enriched genetic algorithms uses four cloud backup servers to restore lost data. The suggested method allows the user to obtain data from any backup server in order to ensure dependability in the event that the primary cloud server fails and is unable to provide users with data. P. S. Challagidad et al (2017). In the event of hardware or software failure, downtime can be reduced by using a method known as disaster recovery. Business continuity is an essential requirement for most businesses. The scholarly literature on cloud computing, catastrophe recovery, and business continuity was examined in this study. The study on cloud computing, disaster recovery, and business continuity was methodically reviewed before a literature search using multiple electronic databases was conducted. However, a thorough grasp of the aforementioned professions' tenets as well as any potential benefits or issues will be beneficial to the information technology industry.(Matar and Fakhri 2016).

Alzahrani et al. (2022) presented an architecture that emphasizes recovery and dependability while combining the advantages of erasure coding and replication to create the best storage solution. In order to validate the data model and provide dynamic structure construction in the future, learning and training techniques were developed.

H5: Information Security awareness (ISA) about safe data backup and recovery can have a favorable impact on the recovery of deleted data.

H6: An effective and practical data recovery plan to recover corrupted, lost, damaged or deleted data can positively affect the security management information's success.system.

4. CONCEPTUAL FRAMEWORK

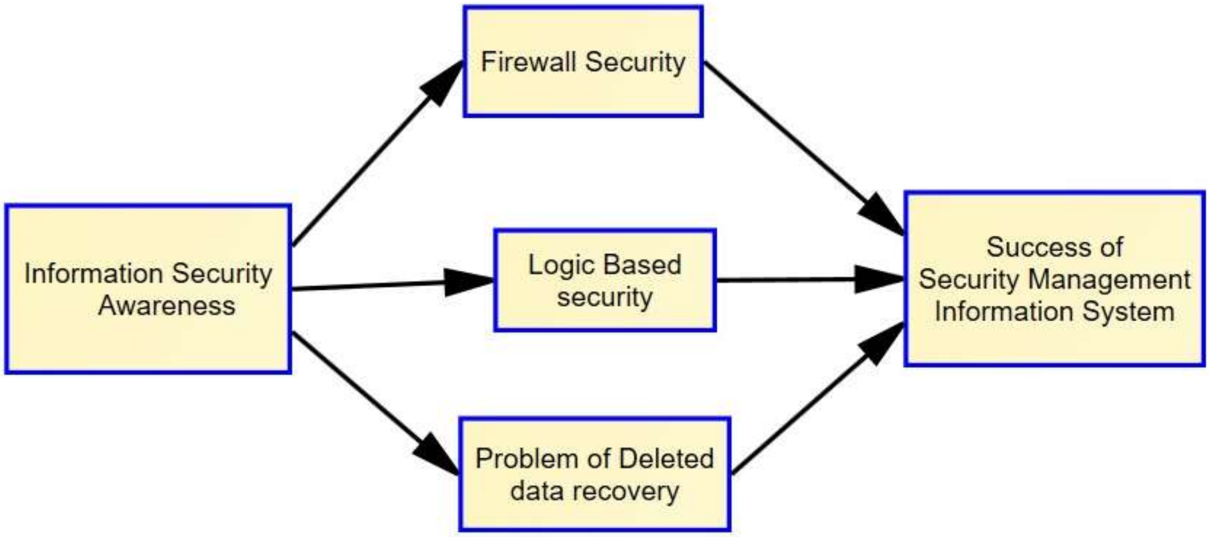
Firewall Security
Information Security Awareness
Logic Based security
Problem of Deleted data recovery
Success of Security Management Information System

Figure 1: Conceptual model proposed assessing the relationship among 'Information Security awareness (ISA)', Firewall security, Logic based security, Problem of deleted data recovery and success of security management information system.

6. CONCLUSION

An in-depth literature review was under taken to identify the factors influencing the success of information security management system. This study created six hypotheses to look into the relationship among 'Information Security awareness (ISA)', Firewall security, Logic based security, Problem of deleted data recovery and success of security management information system. A conceptual model has been proposed assessing the relationship among 'Information Security awareness (ISA)', Firewall security, Logic based security, Problem of deleted data recovery and success of security management information system.

REFERENCES

A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum. Hybrid (2022). Approach for Improving the Performance of Data Reliability in Cloud Storage Management. Sensors, 22(16), 5966. 2022.

A Arul Mary, K. Chitra, (2019)."OGSO-DR: oppositional group search op- timizer based efficient disaster recovery in a cloud environment" J Ambient In tell Human Comput 10, 1885–1895 (2019).

A. D. Rubin and P. Honeyman,(1993). "Long running jobs in anauthenticated environment," in Proceedings of the USENIX Security Conference IV, pp. 19–28, October 1993.

A.. D. Rubin and P. Honeyman (1994) "Nonmonotonic cry ptographicpro to cols," in Proceedings Computer Security Foundations Workshop, pp. 100–116, June 1994.

A. D. Rubin,(1997) “Extending NCP for protocols using public keys, ”Mobile Networks and Applications, vol. 2, no. 3, pp. 227–241,1997.

Agus, Irwan & Destiawati, Fitriana& Dhika, Harry.(2019). Perbandingan Cloud Computing Microsoft On edrive, Drop box, dan Google Drive. Faktor Exacta. 12. 20. 10.30998/faktorexacta.v12i1.3631.

Aktas MS, Astekin M.(2019). Provenance aware run-time verification of things for self-healing Internet of Things applications. Concurrency and Computation: Practice and Experience. 2019; 31(3):e4263. DOI: https://doi.org/10.1002/cpe.4263

Alshammari M.M., Alwan A.A., Nordin A., Al-Shaikhli I.F. (2017).” Disaster recovery in sing lecloud and multi-cloud environments: Issues and challenges”, 4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017, Kuala Lumpur, 2018, vol nr. 2018- Januart, pp. 1-7.

A. M. Matar and A. I. Fakhri (2016). Data recovery and business continuity in Cloud computing: A Review of the Research Literature. Int J Adv Comput Technol, 2016.

Antonelli G, Chiaverini S, Fusco G. (2007).A Fuzzy-Logic-Based Approach for Mobile Robot Path Tracking. IEEE Trans Fuzzy Syst. 2007; 15(2):211–221. DOI: https://doi.org/10.1109/TFUZZ.2006.879998

A. Rathmell. (2001). Protecting critical information infrastructures, Computers and Security 20, p.p 43 – 52.

A. Wool (2004).“A quantitative study of firewall configuration errors,” Computer, vol. 37, pp. 62–67, 06 2004.[Online]. Available: http://www.eng.tau.ac.il/~yash/computer2004.pdf

Baader F, Horrocks I, Sattler U. (2004).Description logics.Springer Berlin Heidelberg; 2004.

Baader F, Calvanese D, Mc Guinness D, Patel-Schneider P, Nardi D. (2003).The description logic hand book: Theory, implementation and applications. Cambridge university press; 2003.

Baader F, Horrocks I, Sattler U.(2005).Description logics as ontology languages for the semantic web. In: Mechanizing Mathematical Reasoning: Essays in Honor of Jo¨rg H. Siekmann on the Occasion of His60th Birthday. Springer; 2005. p. 228–248.

Bamgboye O, Liu X, Cruickshank P.(2019). Semantic stream management framework for data consistency in smart spaces. In: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC);2019. p. 85–90.

Bardis N.G., Doukas N., Markovskyi O.P.(2017),” A Method for Cloud Storage Data Recovery with Limited Loss of Access”, Proceedings - 2017 4th International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2017, vol nr.2018-January,2018, pp.128- 133

Bae WS. (2019). Verifying a secure authentication protocol for IoT medical devices. Cluster Computing. 2019;22:1985–1990. DOI: https://doi.org/10.1007/s10586-017-1107-x

Bobillo F, Straccia U.(2008). An expressive fuzzy description logic reasoner. In: FUZZ-IEEE. Hong Kong, China; 2008. p. 923–930.

Bokhari, S. and Manzoor, S. (2022) Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. American Journal of Industrial and Business Management, 12, 934-954. doi: 10.4236/ajibm.2022.125048.

B. Shojaie and H. Federrath, (2015).“The effects of cultural dimensions on the development of an ISMS based on the ISO 27001,” in 10thInternational Conference on Availability, Reliability and Security,2015, pp. 159–167.

Ciabattoni L, Grisostomi M, Ippoliti G, Longhi S. (2013). A fuzzy logic tool for household electrical consumption modeling. In: IECON 2013. Vienna, Austria; 2013. p. 8022–8027.

Clarke Nathan Steven Furnell, (2012). Power to the people? The evolving recognition of human aspects of security, Computers & Security, Volume 31, Issue 8, 2012, Pages 983-988, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2012.08.004.

D Drives.(2017).”Hard Drive Circuit Board Replacement.“july (2017). [Online].Available: http://www.donordrives.com/pcbreplacement-guide.

Ding-Long Huang, Pei-Luen Patrick Rau, and Gavriel Salvendy. (2010). Perception of information security. Behaviour & Information Technology, 29(3):221–232, May 2010. doi:10.1080/01449290701679361.

D. Newman,(1999). “Benchmarking terminology for firewall performance,” Request for Comments 2647, ftp://ftp.isi.edu/in-notes/rfc2647.txt, Aug. 1999.

D S C Boclin A, de Mello R. (2006). A decision support method for environmental impact assessment using afuzzy logic approach. Ecol Econ. 2006; 58(1):170–181. DOI: https://doi.org/10.1016/j.ecolecon.2005.06.007

Ein-Dor P, Segev E (1978). Organizational Context and the Success of Management Information Systems. Manage. Sci. 24 (10): 1064-1077.

El-Sappagh S, Elmogy M, RiadAM.(2015).A fuzzy-ontology-oriented case-based reasoning framework for semantic diabetes diagnosis.Artificial intelligence in medicine. 2015; 65(3):179–208. DOI: https://doi.org/10.1016/j.artmed.2015.08.003 PMID: 26303105

E. Schultz, (1996). “How to perform effective firewall testing,” Computer Security Journal, vol. 12, no. 1, pp. 47–54, 1996.

F, Bjorck. (2001). Security scandin avian style, interpreting the practice of managing information security in organizations, Stockholm University & Royal Institute of Technology.

Faria H., Solís P., Bordim J., Hagstrom R, (2019).” A backup-as-a-service (BaaS) software solution”, CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science, Brasilia,2019, pp.225-232.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007).Assessing the security perceptions of personal Internet users. Computers & Security, 26 (5), 410–417. doi:10.1016/j.cose.2007.03.001

Galindo J.(2008). Handbook of research on fuzzy information processing in databases.IGI Global; 2008.

Giovanni Vigna, (2000).“A formal model for firewall testing,” http://www2.elet.polimi.it/pub/data/ Giovanni.Vigna/www docs/pub/fwtest.ps.gz.

Haeni, R. (1997, January 1–16). Information warfare: An introduction. The George Washington University Cyberspace Policy Institute.

Hänsch, N., Benenson, Z., (2014). Specifying IT Security Awareness, in: 2014 25th International Work-shop on Database and Expert Systems Applications. pp. 326–330.DOI: https://doi.org/10.1109/DEXA.2014.71

Hussain, M. Z., Hasan, M. Z., Sarwar, N., Nasir, J., & Aslam, N. (2021).Cloud application importance and challenges: A Systematic Review. In 2021 International Conference on Innovative Computing (ICIC), pp. 1-6.IEEE. 2021.

ITU-T (1991).Recommendation X. 800, “Security architecture for Open Systems Interconnection for CCITT applications,” 1991.

ITU-T (2003).Recommendation X. 805, “Security architecture for systems providing end-to-end communication,” 2003.

ITU-T Recommendation X. 509,(2008). “Information technology—Open System Interconnection—The Directory: public-keyand attribute certificate framework,” 2008.

Jaberi, A., Momennasab, M., Yektatalab, S., Ebadi, A., & Cheraghi, M. A. (2017). Spiritual health: A concept analysis. Journal of Religion and Health.https://doi.org/10.1007/s10943-017-0379-z

James HL (1996). Managing information systems security: a soft approach. Paper presented at the Information Systems Conference of New Zealand, 1996. Proceedings.

Jiang H, Chen K, Ge Q, Xu J, Fu Y, Li C.(2021). Data consistency method of heterogeneous power IOT basedon hybrid model.ISA transactions.2021; 117:172–179. DOI: https://doi.org/10.1016/j.isatra.2021.01.056PMID: 33563464

Johnston,A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly,34(3), 549–566.

John D'Arcy & Anat Hovav & Dennis Galletta, (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, INFORMS, vol. 20(1), pages 79-98, March. DOI: 10.1287/isre.1070.0160

J. Zhou and D. Gollmann, (1996). “Fair non-repudiation protocol,” in Proceedings of the 17th IEEE Symposium on Security and Privacy, pp. 55–61, Oakland, Calif, USA, May 1996.

Kamariotou, M.; Kitsios, F.(2023), Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics 2023, 12, 382.https://doi.org/10.3390/electronics12020382

Kankanhalli A, Teo HH, Tan BCY, Wei KK (2003). An integrative study of information systems security effectiveness. Int. J. Inform. Manage. 23(2): 139-154.

Kolokotsa D.(2011). Artificial intelligence in buildings: A review of the application of fuzzy logic. Adv BuildEnergy Res. 2011; 1(1):29–54. DOI: https://doi.org/10.1080/17512549.2007.9687268

Kritzinger E, Smith E (2008). Information security management: An information security retrieval and awareness model for industry. Computers Security, 27(5-6): 224-231.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers and Security, 29(8), 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Lee CC.(1990). Fuzzy logic in control systems: fuzzy logic controller. I. IEEE Trans Syst Man Cybern: Syst.1990; 20(2):404–418. DOI: https://doi.org/10.1109/21.52551

Lee S, Walters S, How lett RJ.(2004). Engine fuel injection control using fuzzy logic. In: 3rd IMechE. Brighton, UK; 2004. p. 287–296.

L. Saleh, (2020). “Cloud Computing Failures, Recovery Approaches, and Management Tools.”In 2020 21st International Arab Conference on Information Technology (ACIT), pp. 1-10.IEEE. 2020.

M.A.M. Stambul & R. Razali, (2011).“An assessment model of information security implementation levels,” in Proc. 2011 Int. Conf. Electr. Eng. Informatics, 2011, July, p. 1–6.

Manjunatha P, Verma AK, Srividya A.(2008). Multi-sensor data fusion in cluster based wireless sensor network susing fuzzy logic method. In: ICIIS-2008. Kharagpur, India; 2008. p. 1–6.

M. N. Alsaleh, S. Al-Haj, and E. Al-Shaer, (2013).“Objective metrics for firewall security: A holistic view,” pp. 470–477, Oct 2013.[Online]. Available: https://ieeexplore.ieee.org/document/6682762 /

Morente-Molinera JA, Pe´rez IJ, Ureña MR, Herrera-Viedma E.(2015). Creating knowledge databases for storingand sharing people knowledge automatically using group decision making and fuzzy ontologies.Information Sciences.2016; 328:418–434. DOI: https://doi.org/10.1016/j.ins.2015.08.051

M. R. Lyu and L. K. Y. Lau,(2000).“Firewall security: policies, testing and performance evaluation,” in Proceedings of the COMSAC. IEEE Computer Society, 2000, pp. 116–21.

M. Satyanarayanan,(1989). “Integrating security in a large distributed system,” ACM Transactions on Computer Systems, vol. 7, no. 3,pp. 247–280, 1989.

N. Freed, (2000). “Behavior of and requirements for internet firewalls,” Request for Comments 2979, http://search.ietf.org/rfc/rfc2979.txt, Oct.2000.

N. Maarop, N. Mustapha, R. Yusoff, R. Ibrahim, and N. M. M. Zainuddin, (2015). “Understanding success factors of an information security management system plan phase self-implementation,” International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, vol. 9, no. 3, pp. 884–889, 2015.

P. S. Challagidad, A. S. Dalawai, and M. N. Birje. (2017). “Efficient and reliable data recovery technique in cloud computing.” Internet of Things and Cloud Computing, 5(1), pp. 13-18. 2017.

P. Williams. (2001). Information security governance, Information Security Technical Report 6 (3), pp. 60–70.

Reda R, Piccinini F, Carbonaro A (2018). Towards consistent data representation in the IoT healthcare landscape. In: ICDH; 2018. p. 5–10. Available from: https://ieeexplore.ieee.org/document/8376515.

R. M. Needham and M. D. Schroeder, (1978). “Using encryption for authentication in large networks of computers,” Communications of the ACM, vol. 21, no. 12, pp. 993–999, 1978.

Rodriguez D, Ezkurdia I, Juan JM, Frankish A, Diekhans M, Harrow J, Vazquez J, Valencia A, Tress ML. (2014). Multiple evidence strands suggest that there may be as few as 19,000 human protein-coding genes. Hum Mol Genet. 2014 Nov 15;23(22):5866-78. doi:10.1093/hmg/ddu309. Epub 2014 Jun 16. PMID: 24939910; PMCID: PMC4204768.

S. Suguna and A. Suhasini, (2014)”Overview of data backup and disaster recovery in cloud,” International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-7, doi: 10.1109/ICICES.2014.7033804.

Saleem, Khizra & Bajwa, Imran & Sarwar, Nadeem & Anwar, Dr & Ashraf, Amna. (2020). IoT Healthcare: Design of Smart and Cost- Effective Sleep Quality Monitoring System. Journal of Sensors. 2020. 1-17. 10.1155/2020/8882378

Sanchez LE, Villafranca D, Fernandez-Medina E, Piattini M (2006). Practical approach of a secure management system based on ISO/IEC 17799. First International Conference on Availability, Reliability and Security, Proceedings, 585-592.

S. E. Chang and C. B. Ho, (2006) “Organizational factors to the effectiveness of implementing information security management,” Ind. Manag. Data Syst., vol. 106, no. 3, pp. 345–361, 2006.

Singh, K.. (2012). Online Data Backup and Disaster Recovery Techniques in cloud computing: A Review. IJET. 2. 249-254.

Siponen M, Willison R (2008). Information Security Management Standards: Problems and Solutions Information and Management.

S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. e. Frantzen, (2003). “Analysis of vulnerabilities in internet firewalls,” vol. 22, 04 2003.[Online]. Available: https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf

S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, (2000). “Implementing a distributed firewall,” in Proceedings of the ACM CCS, November2000, Also see http://www.research.att.com/smb/papers/distfw.html andwww.DistributedFirewalls.com.

Sarwar, Barera & Bajwa, Imran & Jamil, Noreen & Ramzan, Shabana & Sarwar, Nadeem.(2019). An Intelligent Fire Warning Application Using IoT and an Adaptive Neuro-Fuzzy Inference System.Sensors. 19. 3150. 10.3390/s19143150.

Souri A, Norouzi A. (2019). A state-of-the-art survey on formal verification of the internet of things applications.Journal of Service Science Research. 2019; 11(1):47–67. DOI: https://doi.org/10.1007/s12927-019-0003-8

Tang (2018).Xiao bin. Computer Network Security Research [J] Based on Firewall Technology Digital World, 2018(07): 38.

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Bahanag, N. N. M. (2019). Effects of Information Security Management Systems on Firm Performance. American Journal of Operations Management and Information Systems, 4, 99-108. https://doi.org/10.11648/j.ajomis.20190403.15

Tsompanas MAI, Dourvas NI, Ioannidis K, Sirakoulis GC,(2018). Hoffmann R, Adamatzky A. Cellular auto mataapplications in shortest path problem. Shortest Path Solvers From Software to Wetware. 2018; p. 199–237. DOI: https://doi.org/10.1007/978-3-319-77510-4_8

Trillas E, Eciolaza L.(2015). An Introduction to Fuzzy Control. In: Fuzzy Logic An Introductory Course for Engineering Students. 1st ed. Springer International Publishing; 2015. p. 175–202.

Tyagi H, Apergis-Schoute AM, Akram H, Foltynie T, Limousin P, Drummond LM, Fineberg NA, Matthews K, Jahanshahi M, Robbins TW, Sahakian BJ, Zrinzo L, Hariz M, Joyce EM, (2019). A randomized trial directly comparing ventral capsule and anteromedial subthalamic nucleus stimulation in obsessive-compulsive disorder: clinical and imaging evidence for dissociable effects. Biol. Psychiatry 85 (9), 726–734. [PMC free article] [PubMed] [Google Scholar]

Von Solms, B. (2006). Information Security - The Fourth Wave. Computers Security, 25(3): 165-168.

Von Solms B, von Solms R (2004). The 10 deadly sins of information security management. Computers & Security, 23(5): 371-376.

W. Al-Salihy, J. Ann and R. Sures, (2003) “Effectivess of information systems security in IT organizations in Malaysia,” in The 9th Asia-Pacific Conference, 2003, p. 716–720.

Wang X, Fu M, Ma H, Yang Y.(2015). Lateral control of autonomous vehicles based on fuzzy logic. Control Eng Pract. 2015; 34(1):1–17. DOI: https://doi.org/10.1016/j.conengprac.2014.09.015

Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. Journal of Global Information Management (JGIM), 30, 1-16. https://doi.org/10.4018/JGIM.20220701.oa2

Yager RR, Zadeh LA.(2012). Expert Systems Using Fuzzy Logic. In: An introduction to fuzzy logic applicationsin intelligent systems. 1st ed. SSBM, New York, NY, USA; 2012. p. 27–44.

Yang WR, Shiao YS, Su DT, Wang CS.(2002). Design and implementation of fuzzy controllers for autofocus, auto exposure and zoom tracking.JASE. 2002; 11(3):305–312. DOI:https://doi.org/10.6180/jase.2008.11.3.09

Y. P. Baginda, A. Affandi and I. Pratomo, (2018) ”Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE),” 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 2018, pp. 418-422, doi: 10.1109/ICITEED.2018.8534758.

Y. Xu and X. Xie, (2008). “Security analysis of routing protocol for MANET based on extended Rubin logic,” in Proceedings of the IEEE International Conference on Networking, Sensing and Control (ICNSC ’08), pp. 1326–1331, Sanya, China, April 2008.

Y. Xu and X. Xie, (2008). “Extending rubin logic for electronic commerce protocols,” in Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification (ASID ’08), pp. 448–451, Guiyang, China, August 2008.

Y. Xu and X. Xie,(2008) “Analysis of authentication protocols based on rubin logic,” in Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM ’08), Dalian, China, October 2008.

Y. Xu and X. Xie, (2008). “Analysis of electronic commerce protocols based on extended rubin logic,” in Proceedings of the 9thInternational Conference for Young Computer Scientists (ICYCS’08), pp. 2079–2084, Hunan, China, November 2008.

Zhong R., Xiang F.,(2012).” A cost aware backup strategy in hybrid clouds”, Proceedings - 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2012, Beijing, 2012, pp.256-260.

Zuccato A (2007). Holistic security management framework applied in electronic commerce. Computers Security, 26(3): 256-265.