Scientific Research Publishing

Journal of Information Security, 2018, 9, 315-333
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

# Ontology-Based Cyber Security Policy Implementation in Saudi Arabia

**Amir Mohamed Talib, Fahad Omar Alomary, Hanan Fouad Alwadi, Rawan Rashed Albusayli**

College of Computer and Information Sciences, Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, KSA

Email: ganawa53@yahoo.com, fahd.alomary@gmail.com, shalajmi@hotmail.com, rbusayli@imamu.edu.sa

**How to cite this paper:** Talib, A.M., Alomary, F.O., Alwadi, H.F. and Albusayli, R.R. (2018) Ontology-Based Cyber Security Policy Implementation in Saudi Arabia. *Journal of Information Security*, **9**, 315-333.
https://doi.org/10.4236/jis.2018.94021

**Received:** September 4, 2018
**Accepted:** October 23, 2018
**Published:** October 26, 2018



## Abstract

Cyber security is an important element of national security and the safekeeping of a nation's constituency and assets. In Saudi Arabia, the point of interest on cyber security is particularly outstanding due to the fact that Saudi Arabia has a highly cyber attacks all over the Arab countries. This paper displays on contemporary studies done in Saudi Arabia in regards to cyber security policy coverage. The point of interest of this paper is the use of ontology to identify and suggest a formal, encoded description of the cyber security strategic environment, and propose the development of ontology to be able to permit the implementation of the sort of policy. The intention of the ontology is to become aware of and constitute the multi-layered company of gamers and their related roles and obligations within the cyber security environment. This could make contributions in large part to the improvement, implementation and rollout of a country wide cyber security policy in Saudi Arabia.

## Keywords

Cyber Security, Cyber Security Policy, Implementation, Ontology, Saudi Arabia

## 1. Introduction

Information and its associated infrastructures are fundamental to cyber security and the implementation of associated cyber security coverage. On the other hand, cyber security relates to the renovation of countrywide security and the hobbies of citizens; even as, however, it may confer with politically encouraged hacking to conduct sabotage and espionage against precise country states. Consequently, the motive in the back of countrywide cyber security is to permit the safekeeping of a country's constituency and its related organizational, human,

economic, technological and informational sources. That is finished to facilitate the fulfillment of its country wide targets [1].

In Saudi Arabia, cyber security has been diagnosed as a critical component contributing toward country wide safety. Extra geographical regions of Saudi Arabia are becoming integrated into the worldwide village, necessitating additional authorities projects aimed at bridging the virtual divide and addressing cyber security. One of these initiatives is the development and implementation of a Saudi Arabia precise cyber security policy.

This paper looks at the cutting-edge and future studies and improvement carried out in the direction of the implementation of cyber security coverage in Saudi Arabia. It's going to gift retrospective reflections, in addition to proposed destiny paintings on selected methodologies and frameworks with a purpose to enable the implementation of this kind of policy. The revolutionary contribution of this research lies in the argument that ontology can assist in defining a version that describes the relationships between different cyber security additives.

This research has been driven from different institutions, colleges, public and private companies, and universities inside KSA (Kind Abdul-Aziz University—Saudi Arabian Oil Company (Saudi Aramco)—Umm Alqura University—King Faisal University—King Abdulaziz City for Science and Technology—King Saud University—Taibah University—Prince Sultan University—King Fahd University of Petroleum & Minerals—University of Tabuk—Alfaisal University—University of Dammam—College of Technology of AL Kharj—Princess Nourah Bint Abdulrahman University—Jazan University—Qassim University—Qassim Private Colleges—Yanbu University College—Effat University—Communications and Information Technology Commission—Saudi Arabian Monetary Authority) to understand which cyber security policies have implemented.

## 2. Background

Saudi Arabia, officially known as the "Kingdom of Saudi Arabia (KSA)", is one among Gulf countries situated in western Asia. It's miles absolute monarchies, governed by means of huge family. Arabic and Islam are the principle language and religion of this country. From an monetary perspective, in conjunction with the other nations in the Gulf countries, Saudi Arabia rely heavily on oil and offer two-thirds of the sector's oil [2] [3]. As a consequence, authorities and government security in terms of the sector's largest wellspring of crude oil assets is extremely crucial.

Given the modern-day popularity of the policy framework in Saudi Arabia, it is agreed that there isn't always sufficient emphasis at the countrywide cyber security coverage, despite the fact that references is made to the coverage because the overarching method that ought to manual cyber security. In response, this paper proposes 11 policies as a foundation for the Saudi Arabia cyber security policy requirements: 1) security identification of threats, 2) security awareness, 3) security assurance, 4) confidentiality, 5) integrity, 6) availability, 7) privacy, 8)

authentication, 9) authorization, 10) access control, and 11) trust.

It is recommended that those 11 policies must be present in growing a national strategy for a powerful cyber security approach and policy. The following phase addresses those elements in greater detail, with an initial mapping of current Saudi Arabia cyber security research to determine the current nation and development of a cyber security coverage implementation. These factors match with the Saudi Arabia proposed multi-faceted technique to lessen cyber crime.

## 3. Current Researches Concerning Cyber Security in Saudi Arabia

The dynamic and volatile nature of the internet and the cyber area in fashionable makes cyber security studies inside Saudi Arabia an essential region to cope with. Because the cyber area is inherently globalized, it can't honestly be considered in isolation or on a in basic terms country wide foundation. With this in mind, the 11 policies identified above as a part of the success development of a national cyber security method are discussed next, when it comes to modern Saudi Arabia research.

### 3.1. Critical Security Factors That Influence the Decision of Cloud Adoption

Alassafi *et al.* [4] stated complications regarding the adoption of cloud technology in Saudi government agencies with a proposed security factors framework. The framework consists of security risks factors, security benefits factors, and social security factors that influence the decision to use cloud-based services in Saudi Arabia. The authors used triangulation validation method which involves three phases to investigate and validate the framework factors. The first phase, data were collected from desk research by an intensive review of related works. The second phase, twelve experts were interviewed to critique the proposed framework and confirm it. A questionnaire with closed-end questions was distributed to IT and security experts who have experienced cloud technology in five Saudi government agencies, and it was the final phase.

### 3.2. Key Factors of Successful Sustainable Development

Sustainable development in information technology has critical factors that influence its success. Saeed Bawazir from Saudi Arabia Oil Company—Aramco—has conducted research addressing these factors in details [5]. The author has mentioned the role of Saudi Arabia in making significant contributions to sustainable development by implementing e-Government services and adopting information technology practices. The e-sustainable solutions have a positive impact on the environment, and many benefits can be gained; however, many challenges are raised such as maintaining security. The security in e-Government has to be investigated carefully on different levels to maintain the success of such a transition. Strategic level, process level, interaction/user level, and data and information level are the bases for organizations to accomplish security on their systems.

The author has emphasized the need for further research in the security field to save the government agencies from breaches and attacks [5].

### 3.3. Adherence to ICT Security and Privacy Policies

Saudi Arabia government attitude toward security and privacy policies in comparison to Australia and the United Kingdom has been studied by [2]. The study shows a lack of readiness policies, practice such policies, and the principle of rewards and sanctions to achieve compliance with security and privacy policies compared to the other two countries. The level of awareness of information security is shallow among the employee in Saudi Arabia public enterprises. One study shows almost half the staff members are unaware of privacy policies related to their department. Policies in Saudi Arabia are not linked with specific actions and considered by judicial proceedings by the Bureau of Investigation and Public Prosecution. This method is not sufficient compared to what has been conducted in Australia and the United Kingdom. They assign each article of the policies to the relevant government department and convert the article to actions to be practiced by the staff. They use penalties and rewards to punish who make mistakes and encouraging who adhere to these policies. Saudi Arabia is working on the principle of sanctions but has not practiced the rewards principle due to the gap in measuring the policy implementation in government organizations. The Saudi government has to take further steps to enhance the adhesion to security and privacy policies such as providing education and training to the employees to leverage their awareness level [2]. A budget has to be supported to the public enterprises to create, implement, and evaluated the security and privacy policies. Supply chain products have to be compatible with security and privacy requirements to ensure proper implementation of security and privacy policies.

### 3.4. A Hybrid Approach to Developing Cyber Security Ontology

Ontologies rely on one of the two approaches either human expert who works if the desired ontology is small to easily containment their communications or by a computer which can read as human read. The latter approach cannot be entirely successful except if the machine passed Turing Test which is not possible with the current technology. The difficulties surrounding these methods to produce cybersecurity ontology led Geller *et al.* to introduce a tool which maximizes support for human experts to build the required ontology by minimizing the communication between experts who work on different modules [6]. The developed device which is called Security Knowledge Acquisition Tool (SKAT) combines experts' manual extension to security terms with Bootstrap Ontology—index terms classifier. The semi-automatic approach uses previously classified textbook index terms as input into a seed ontology of concepts. The unclassified terms are then shown to the experts to manually place them into the ontology after identifying their occurrences by Concept Recommendation compo-

nent. The tool has been available to two domain experts and the authors still receiving feedbacks regarding their tool usability and utility.

### 3.5. Security Issues Concern for E-Learning by Saudi Universities

E-learning is adapted by Saudi Arabia to provide a proper infrastructure for education [7]. This adoption has increased the number of registered students and has given them a chance to learn conveniently at their own pace. However, the students' information availability online creates more threats and attacks for E-learning platforms security. The primary security concerns are varied starting from user authorization and authentication and ending with data integrity and non-repudiation. Ahmed *et al.* [7] have proposed some countermeasures that can be taken by Saudi E-learning providers to counter security threats related to user identification and authentication services. The Short Message Service (SMS) Information Security, Biometrics Information Security, Token Based Information Security Mechanism, Access Control List (ACL) Mechanism, Digital Signature Information Security Mechanisms are practical applications to protect data and maintain security and privacy to Saudi students. Passive and active attacks have to be considered, and prober cryptographic algorithms have to be designed and implemented to preserve students' data.

### 3.6. Healthcare Data Security in Cloud Computing

Electronic health records (EHRs) allow healthcare providers, insurance companies and patients to access and manage patients' profile easily with no restrict to time or place. However, due to the unpredicted volume and heterogeneity of these medical records, moving them to cloud platforms becomes a necessity. Cloud computing technology represents a significant reduction in processing power and time, but security risks need to be considered carefully by cloud providers to satisfy healthcare regulations regarding the security and privacy of patients' information. Elmogazy and Bamasak introduce a centralized, secure data sharing framework that ensures the data confidentiality, authentication, integrity, and availability in a multi-level hierarchical order based on fully homomorphic encryption (FHE) and Attribute-Based Encryption (ABE) algorithms [8]. A combination of the latter encryption algorithms is used to encrypt all EHRs, and an index search algorithm is used before moving the data to the cloud. The records are divided into two parts one portion that can only access by only legitimate users through identification and authorization. The other portion of the EHRs can be accessed if the healthcare provider gives the information seekers such as researchers access privileges which depend on their needs. The framework is in the development stages, and the results have not been published [8].

### 3.7. Secure Data Aggregation in Wireless Sensor Networks

A wireless sensor network (WSN) incorporates scattered tiny sensors over a sensing field which equipped with specific tasks such as measuring the tempera-

ture, sensing movements, etc. One of these sensing nodes is called sensor mote which reduces the pardon over the base station. It aggregates data from different sensors and sends the results to the upper-level node or the base station instead of each node sends data to the base station. Securing data aggregation has been an attractive topic, and many solutions and protocols were proposed by researchers to solve presented security risks. Othman *et al.* have introduced an algorithm which uses homomorphic encryption and Message Authentication Code (MAC) to tackle the security risk of forged aggregation results [9]. The proposed algorithm shows a significant reduction in the computation and communication overhead that plays a vital role in sensors energy consumptions.

### 3.8. Integrity Protection of Software for E-Health Data

Modifying the binary source of an application allows an attacker to manipulate the produced data. E-Health environments are exposed to the problem of unprotected and altered software that works for the favor of the attackers which could change or disclose patients' data. Rahman from King Saud University has proposed a light-weight cryptographic methodology that alleviates the problem of unauthorized changes to program flows [10]. A secure cryptographic signature is computed for both static and dynamic code tempering protection. The static code tempering is done before running the software and can be verified by comparing the current calculated cryptographic signature with the previously generated cryptographic signatures. The dynamic tempering happens during the execution of the software by using unprotected memory. This attack can be caught by dividing the application into modules with a specified length and compute the cryptographic signatures for each module. The secure cryptographic signature is kept in a signature file which is used for verification with the running program. The results show the success of the proposed method to detect forgery activities mainly on the application running state.

### 3.9. Game-Theoretic Algorithm Stimulating Cooperation in Multi-Hop Wireless Networks

Baig *et al.* [11] demonstrate the problem of selfish nodes in a wireless sensor network (WSN) and proposed a novel distributed game-theoretic algorithm that motivates cooperation among these nodes. The nodes in the wireless network are limited in their resources, and due to the absence of unified control center, the nodes have no incentive to participate. This selfishness has a significant impact on the network performance and increases the number of dropped packets by affecting their routes. The authors present a model that based on alternating prisoner's dilemma (APD) which uses interaction history of a node with its neighbor nodes to stimulate the cooperation among nodes. Since nodes communicate through wireless media, the noise and packet collision are possible, and the proposed algorithm effectively consider these circumstances not unfairly to punish the node. The algorithm testing results show its robustness against two of well-known and strong strategies called Tit-for-Tat (TFT) and PAVLOV.

### 3.10. DDoS Attacks and Countermeasures in Cyberspace

Two ways can be used to run a denial of service (DoS) attacks; either by exploiting internet model protocols' vulnerabilities or direct excessive illegitimate traffic to a targeted system to deny access from intended users. The DoS attacks increase system's resources consumption to prevent intended users from using them and get the system down. Distributed Denial of Service (DDoS) attack has the same mechanisms, but multiple sources are involved, which complicate the problem and make defense mechanisms harder. Zeb *et al.* [12] have given a detailed study of these attacks, their defending and mitigating methods, and challenges surrounding defense mechanisms mainly on TCP/IP internet protocol. The research shows a need for an upgrade on the used hardware in the global network infrastructure, and more integrated solutions have to be developed in the software level.

### 3.11. SDTP: Secure Data Transmission Protocol in Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs) contain two parts: wireless communications and nodes. The nodes (PCs, Mobile device, printers, etc.) are self-organized which connect themselves with each other using Ad Hoc network. MANETs' characteristics make them vulnerable to security attacks as they have dynamic topology, infrastructure-less, and many other challenges. Faisal and Mathkoor [13] have proposed a new protocol called Secure Data Transmission Protocol (SDTP) to ensure confidentiality, integrity, authentication, and availability of transmitted data in ad hoc networks. The protocol takes advantage of multi-paths routing between nodes to enhance security by establishing disjoint-multiple paths between a single source node and a single destination node. Trust model and key management model have been integrated into SDTP to generate and validate keys and certificates. The confidentiality achieved through end-to-end encrypted messages that distributed in multiple shares. The authentication and integrity are checked on shares. The availability is implemented using acknowledgment technique and redundancy in the shares.

### 3.12. Digital Watermarking to Preserve Integrity of the Digital Holy Quran Images

Digital Quran is unprotected which makes intentional or unintentional tempering to Quran's verses unavoidable. Holy Quran content's integrity is essential to Muslims and preserving its authenticity is an emerging issue. Recent studies show watermarking approaches effectiveness in detecting any changes to an image which Kurniawan *et al.* [14] take this approach to protect the integrity of Quran' images. The proposed solution uses Discrete Wavelet Transformation (DWT) to bring input image to fragile watermarking that embed watermark using spatial and frequency domain. The experimental results show the method robustness to brute-force, collage, and local attacks. Besides, it can afford acceptable tampering localization at a minimum watermark payload with fine im-

age quality.

### 3.13. Techniques to Preserve the Integrity of the Electronic Versions of the Nobel Quran

Another tool has been presented by Alsamdi [15] that ensure the integrity of the wording in the Quran based on hashing mechanisms. The system uses information retrieval techniques to look for verses and compute their hashes with the original ones to validate their integrity. The conducted experiments have proven its success as automatic authentication process with limitation to different Quranic readings.

### 3.14. Security Model for Cloud Database as a Service (DBaaS)

Munir [16] proposed a security model for Cloud Database as a service (DBaaS) that ensure its confidentiality, privacy, integrity, and availability. The model discusses security matters in four different layers. The first layer—user interface layer—uses Single Sign-on Authentication to authenticate a legitimate user. Access controls are used in the second layer which mainly gives access to software services and storage space on the Cloud. Efficiency and reliability are presented in the third layer as it allows for query statements reusability and reliable management services to the database. The Fourth layer is the actual data storage which is responsible for data encryption and decryption, data integrity, and data recovery. The approach has dealt with different security issues related to the DBaaS which are based on traditional techniques. However, a need for more improvement is essential to make these techniques more mature, practical and reliable for securing Cloud database services.

### 3.15. A Model for Securing Islamic Websites: Formal Specification Paradigm

Abuhaija *et al.* [17] suggest a universal security model for websites authentication and content integrity. The authors plan to build a trusted Web sites directory for Islamic websites called Islamic trust (ITRUST) that offer Islamic researchers from Arabic and non-Arabic speakers genuine and credible material about Islam. The primary objective of the developed formal specifications for the proposed architecture is to ensure the trustworthiness of Islamic websites. Also, protect Muslims and Non-Muslims from accessing websites that have misleading and incorrect Islamic data. The proposed architecture framework contains five main entities: Content Provider (CP), Registration Authority (RA), Watermark Service Provider (WSP), Judge Authority (JA), and Layman users. The system is under development and testing, and more work is planned to be done before reaching the final product.

### 3.16. An Identification and Prevention of Theft-of-Service Attack on Cloud Computing

Investigate the limitations of KVM hypervisor with QEMU emulation technique

to prevent theft-of-service attack that allow user to use the VM for a longer period for hostile or general actions. In addition, propose and implement an API, which can identify and prevent theft-of-service attack by using power consumption's statistics of a VM, residing on external cloud, as well as alert the administrator during attack. The solution in details, it is calculating power consumption during different intervals of time so that use the calculated power consumption of VM (through our API) being used by an attacker. Later, an API can compare the calculated power consumption of VM, from external cloud, with the manipulated power consumption (where attacker resets the variables and show no usage of VM), calculated by primary cloud. If there is a difference in power consumption taken by primary and external cloud, either API alerts the administrator or consider the values from external cloud to charge user [18].

### 3.17. Secure Data Aggregation Scheme in Wireless Sensor Networks for IoT

Alghamdi *et al.* [19] presents a secure data aggregation scheme in Wireless Sensor Networks for IoT. The proposed method encrypts the sensor data by elliptic-curve based seed exchange algorithm and Hilbert curve based data transformation. The privacy-preserving scheme is performed through three phases. Network construction phase: Message sent between two parties. The message exchanged between sink and Sibling nodes. Data encryption phase: generates random seed data using elliptic key, which is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. It requires smaller keys compared to non-ECC cryptography to provide equivalent security. Data aggregation phase: each node sends the encrypted data to its parent node. Then, the parent node analyses the encrypted data of the performance evaluation analysis of this approach by using the PowerTossim extension.

### 3.18. Extended Grouping of RFID Tags Based on Progressive Edge-Growth Methods

Alkanhel and Ambroze [20] proposes a novel method for recovering missing radio frequency identification (RFID) tag identifiers from a group, based on progressive edge-growth (PEG) methods. Extended grouping of RFID tags allows the recovery of missing tag identifiers without external systems such as databases. Motivated by the properties of Tanner graphs, or equivalently, parity check matrices constructed using PEG methods. In addition, this paper examines the performance and complexity of Gaussian elimination (GE) and iterative (IT) decoding algorithms. Since the memory space in RFID tags is limited, it used a hash function is applied to a group of tag identifiers to obtain the digest value instead. It studies group integrity checking without external systems. The resulting digest value is treated as a group identifier and recorded on all tags in the group. This process is called coupling or grouping in some papers. Once a group is formed, group integrity checking is performed by reading all tag identifiers from a given group having the same group identifier. Then, a hash function is

applied over the reading tag identifiers, and the computed hash value is compared with the stored group identifier. If there is a mismatch, the group integrity is invalid, meaning that one or more tags are missing; otherwise, the group preserves its integrity. Even though the method presented in enables fully autonomous group integrity checking, it is not able to recover the missing identifiers.

### 3.19. Preventing and Securing Data from Cyber Crime Using New Authentication Method Based on Block Cipher Scheme

The proposed method of preventing data against cybercrime based on block cipher scheme [21]. Encryption and decryption techniques method in the block cipher algorithm using in the form of message blocks. The message or plain text divided according to the selected type of block cipher model. The block cipher packet transmits through communication channel to the recipient end for decrypting procedure using private key or public key. Therefore, cybercriminals are unable to modify or stealing of data. We have process Securing the data scheme have 3 stages of process; first is key generation(calculate inverse of det value and minor elements with matrix elements, then mod 37, the reminder value is the private key), second encryption using formula (Cipher Text = (key × message × any integer value) mod 37) and another decryption(Evaluate with encrypted message using Private Key Then value of remainder using modulo 37 is called as (Senders message) stages. considered various security aspects that should be taken into justification in depth in order to have suitable data privacy and security on open and wireless Channels [21].

### 3.20. Low-Latency Hardware Architecture for Cipher-Based Message Authentication Code

Dhaou *et al.*, [22] proposes a low-latency architecture for the CMAC algorithm using 128-bit AES processor. The architecture uses LUT for parallel implementation of the critical blocks, SubBytes and MixColumns, and uses BRAMs for Sbox and expanded keys. Further, the paper described synthesis results for both AES and CMAC obtained using low-power Virtex-6 FPGA. The results show that our architecture has the lowest latency compared with state-of-the-art implementations.

### 3.21. A Lightweight Authenticated Encryption Scheme Based on Chaotic SCML for Railway Cloud Service

Zheng *et al.* [23] proposed railway application supported by cloud computing are based on the resources from an integrated data center, which collects massive railway infrastructure data through the dedicated mobile-IoT-cloud-network in real-time. As a result, there is a growing demand for an efficient and secure IoT network to protect the data stream. In the IoT-cloud-based intelligent railway, data are inseparable with automated operation and maintenance; therefore, the integrity that protects the data from unauthorized manipulation and the confidentiality that prevents leakage of sensitive information is critical to the net-

works. Thus, the encryption algorithms and the message authentication codes are widely used together. It introduces an on-line authenticated encryption system based on hardware implementation, which is designed and simulated through VHDL.

### 3.22. Securing RPL-Based Internet of Things Applied for Water Pipeline Monitoring

Elleuchi *et al.* [24] uses several security techniques to protect control Messages (DODAG Information Object (DIO), Destination Advertisement Object (DAO) and DODAG Information Solicitation (DIS)) of RPL (Routing Protocol for Low-Power and Lossy Networks) while respecting energy constraints of the IoT devices. The security techniques and algorithms used in IoT should protect the exchanged messages between sensor nodes from attacks and then achieve security requirements, which are integrity, confidentiality, availability, and authentication. The proposed solution minimizes the impact of several types of routing attacks as sinkhole, wormhole and Sybil and prevents lies and modifications. It is based on using IBC to generate pairwise keys and AES 128 and SHA 256 protocols to generate MACs. To evaluate memory and power consumption overhead of our proposal, we use COOJA simulator on CONTIKI operating system.

### 3.23. Web Application Development Model with Security Concern in the Entire Life-Cycle

Shuaibu and Ibrahim [25] proposes a tool by selection of web development framework from existing web development frameworks as well as building new security framework with checks and balances around the web development framework. Developing a prototype from the new security framework and testing the prototype based on security concerns. The Second category involves evaluation phase for the new security framework with the existing security frameworks for web application using an experiment method known as within subject design proposed security model considers security at early and throughout the entire life-cycle of web application development although the model is based on Extreme Programming.

### 3.24. Mobile Fingerprint Authentication in Saudi Arabian Call Centers

To reduce the fraud rates and leakage of sensitive information, reported by customers. In this Context, the usage of biometric-based authentication systems, e.g. fingerprints, face recognition, etc. is exponentially growing in the call centers [26]. This work focus on the design and development of mobile-fingerprint based authentication system for call centers. The devised system reduces frauds and safeguard customers sensitive data. It verifies callers' identity without dealing with the tedious processes of verifying PIN numbers and other methods currently adopted by conventional. Call centers. Mobile fingerprint devices are employed to verify the authentication of each caller. The call center system will

be integrated with the fingerprint scanner feature that already exists in smart phones to authenticate callers before providing any service.

### 3.25. Information Security Policies and Procedures Development Framework for Government Agencies

Government Agency, developing a single policy document that speaks to all types of users within the organization and addresses all the information security issues necessary may prove impossible [27]. A more effective concept is to develop a suite of policy documents to cover all information security bases; these can be targeted for specific audiences, making a more efficient process for everyone. This Framework examines the elements that need to be considered when developing and maintaining information security policies and procedures and goes on to present a design for a suite of information security policies and procedures documents and the accompanying development process. It should be noted that there is no single method for developing an information security policies and procedures. Many factors must be taken into account, including audience type and Government Agency business and size [27].

### 3.26. Information Security Policy for E-Commerce in Saudi Arabia

Thakur *et al.* [28] carried out a study to determine the efficiency of the project and suggested that out of the existing 22 ministries in the kingdom implement feature of E-government in their online websites. 10 ministries were either completely or partially in the first stage of implementing the project, which was defined by establishing E-government features in their websites. Defined by a one-way interaction between the ministries and the citizens, development and implementation of security control systems for information systems plays an important part in ensuring that the operations and service delivery mechanisms by any government agency are achieved in the most efficient and effective manner. Security controls are the management, operational and technical safeguards employed in the information systems to sustain information and data integrity, confidentiality and availability.

### 3.27. Academic Integrity: Saudi Students Perspective

Student academic dishonesty is the social pressure demanding them to demonstrate productivity performance, and speed encourage faculty to articulate their policies toward academic misconduct and it stated consequences for students [29]. To solve the problem of dishonesty, faculty raise students' ethical awareness to decrease the frequency of cheating Students cheat due to social pressure these pressures through providing peer support, more learning support systems specially for international students, and progress check points along the academic courses may decrease the amount of academic pressure they suffer and may also decrease their fear of failure alleviating their social threats. Instructors should focus on knowledge not grades.

### 3.28. Cyber Security Framework for Saudi Arabian Monetary Authority

It uses cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats [30].

### 3.29. Security Risk Factors That Influence Cloud Computing Adoption in Saudi Arabia Government Agencies

The proposed framework is intended to investigate the security risk factors that influence the adoption of cloud computing in Saudi Arabian context [31]. This framework proposed the successful adoption of cloud computing focused on risks when implementing security in the cloud system. Focus on the security risk factors that affect government agencies decision to adopt the cloud. This study is aimed to construct a framework to investigate the cloud security risks and the cloud security features that influence Cloud Computing adoption in Saudi Arabia.

### 3.30. The Influence of Students' Knowledge on Security towards Their Behavior with Security Risks within the Context of Saudi Arabia

The authors are develops the level of awareness regarding the main security issues. The major security issues that had been asked were related to copyright and piracy viruses, firewall, passwords, backup, public network and software issues [32]. Students show good and safe behaviors with email are aware to culture (copyright culture and ethics).

## 4. Ontology: Definition

Grüber [33] defines ontology as "formal, express specification of a shared conceptualization". A formal ontology specifies a device-readable domain version depicting entities and their inter-entity relationships. It commonly consists of a descriptive part and reasoning technology. The descriptive a part of ontology captures the domain from the area experts' factor of view, expressing area records in a manner that can be processed through computer systems and be understood by way of people. Using reasoning technologies enables new information to be derived from the information contained in ontology.

In this research, Web Ontology Language (OWL) is chosen to represent cyber security policy because of its power to express meaning and semantics and complex relationships. This section gives a very broad overview of OWL to assist readers in understanding the following sections. Readers that are familiar with OWL concepts should skip this section. Readers that are interested in further details of OWL should refer to [34] for additional information. The basic concepts in OWL are classes, individuals and properties. The basic construct in

OWL are classes. Classes describe concepts in the knowledge domain. Properties can further define relationships between classes, constrain classes or describe various attributes of classes. There are two types of properties: object properties and data type properties. Object properties relate instances of one class to instances of another class. Data type properties relate instances of a class to Resource Description Framework (RDF) literals or XML Schema Data types. There are lots of characteristics that make Protégé a considerable selection for our proposed ontology. Protégé helps ontology development, using text mining and natural language processing to extract relevant terms from the scientific literature that can then be organized, Protégé allows vocabulary designers to capture, refine and ultimately formalize their intuitions without being forced to deal with distracting logical details early in the design process.

## 5. Using an Ontology in Implementing Cyber Security Policy in Saudi Arabia

The 11 policies that driven from the current researches concerning cyber security policy implementation in Saudi Arabia show that some efforts have been made in mapping of Saudi Arabia research and development activity. But, since not all cyber security policy are bounded and defined, however, it is very difficult to ensure an easily implementable cyber security policy.

The contributions that could be driven from this section are:

- This paper proposes an ontology development in the era of security policy implementation in Saudi Arabia along with functions and responsibilities.
- This paper also clears the complexity the structure necessarily and formal description of the environment before implementation of the coverage can succeed.
- Ontology will provide a site mapping of a shared environment between a cyber security domain and relevant entities and functions of the proposed 11 cyber security factors that implemented in Saudi Arabia.

## 6. Cyber Security Policy: Ontology Domains

The best benefit of implementing ontologies in the domain of cyber security policy implementation in Saudi Arabia is that the authors will be easy for them to identify and propose a formal and encoded the descriptions of the cyber security policy environment. The cyber security policy implementations in Saudi Arabia ontology are:

- **To share common understanding of the structure of information among people:** due to the dynamic and unstable nature of the cyber security area, there are regularly more than one explanations or ambiguous understandings of area particular concepts. Ontology will assist in standardizing these ideas.
- **To enable reuse of domain knowledge:** there are many role players in Saudi Arabia which have performed studies and development work on cyber security. Regarding these functions gamers as area specialists in the development

of the ontology will maximize the utilization of any current domain expertise.

- **To make domain assumptions explicit:** making explicit domain assumptions underlying an implementation makes it viable to alternate those assumptions easily if our information about the domain changes.
- **To separate domain knowledge from the operational knowledge:** with the aid of the use of ontology, it would be feasible to make sure integration and interchangeability among exceptional components of the bigger Saudi Arabia cyber domain.
- **To analyze domain knowledge:** present area knowledge, once diagnosed and captured within an ontological model, may be used to finalize the Saudi Arabia cyber safety coverage, and implement its components to ensure the better protection of national security and safekeeping.

This paper illustrates a high-level ontology development of cyber security policy. The ontology based on cyber security policy is implemented using "Protégé", which is a free and an open source platform that implement a suitable tool constructs knowledge based models and applications with ontology model. Figure 1 illustrated the main entities, attributes and their relationships of cyber security policy.

The main entities are implemented here in this ontology that consists of the cyber security policy types which are: Acceptable Use Policy, Password Policy, Encryption Policy, Confidential Data Policy, Retention Policy, Incident Response Policy, Guest Access Policy, Email Policy, Virtual Private Network (VPN) Policy, Third Party Connection Policy, Backup Policy, Outsourcing Policy, Network Access Policy, Data Classification Policy, Network Security Policy, Physical Security Policy, Wireless Policy, Mobile Device Policy, and Remote Access Policy.

The main attributes are implemented here in this ontology consists of: goals and plans of cyber security policy, which are compromised to be as a target.

## 7. Conclusions and Future Works

This paper highlights the cyber security policy implementation in Saudi Arabia, summarizes progress made up to now of the studies and improvement completed, and proposes the way ahead. The authors talk the necessities in an effort to enable the implementation of the cyber security policy and reflect on studies that are presently being carried out on using an ontology on this regard. The intention of the ontology is to begin with to offer a formal description of position players and their function inside the cyber security environment. Despite the fact that numerous research articles and initiatives have been undertaken throughout the last 5 years, handiest restrained studies have been achieved on the implementation of the cyber security policy implementation coverage in Saudi Arabia.

The future works will be extended from this research include:

- Formalize an implementation framework of cyber security policy in Saudi Arabia.

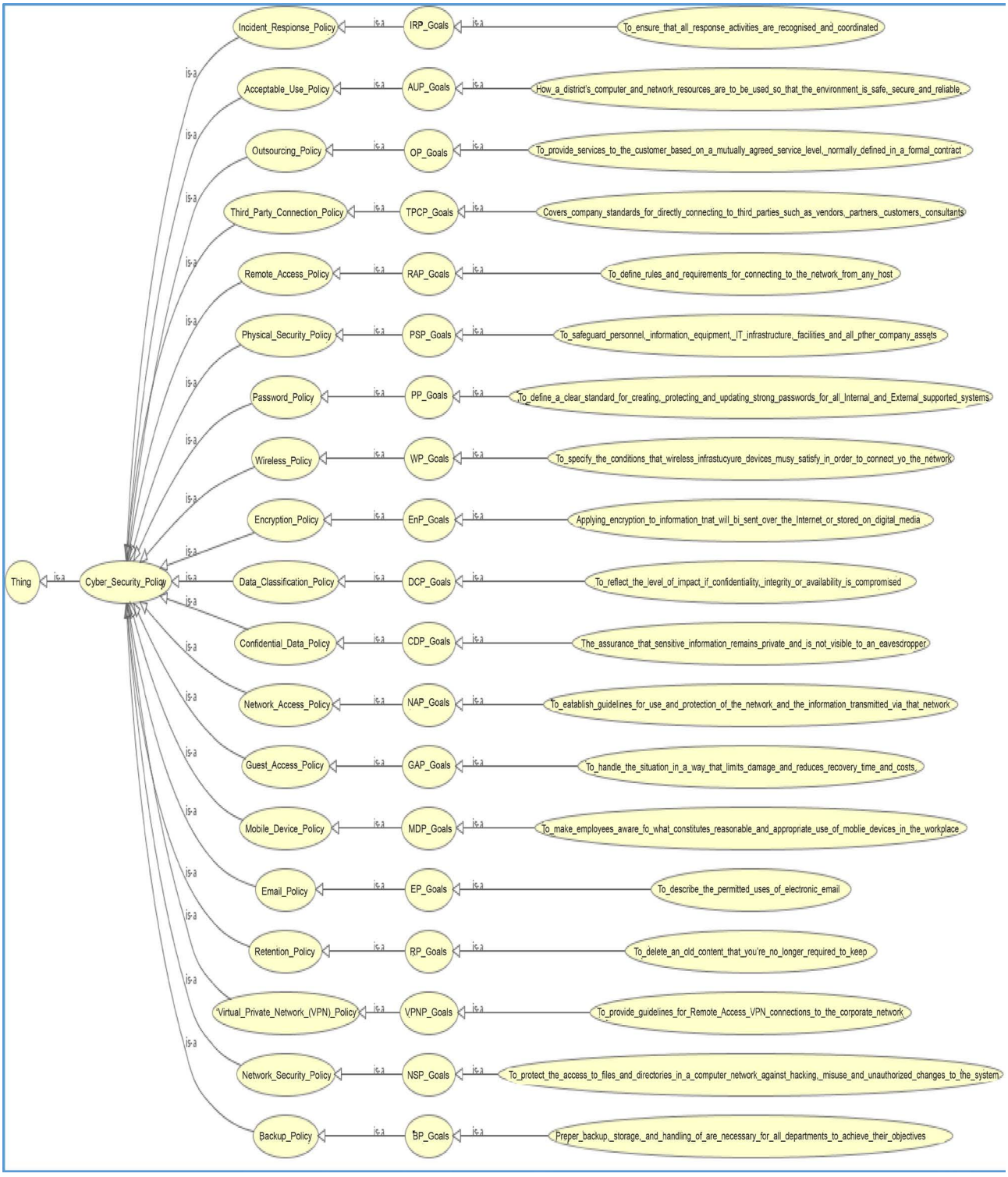


**Figure 1.** Cyber security policy ontology illustration.

- Analyze the differentiation between the security components and security policies in Saudi Arabia.
- Define the organizational structure development necessary for cyber security policy is a good way to determine the strategies so that it will reap the recog-

nized objectives of the policy.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References


[1] Ghernouti-Helie, S. (2010) A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 *International Conference on Availability, Reliability and Security*, Krakow, 15-18 February 2010, 370-373. https://doi.org/10.1109/ARES.2010.119

[2] Almarhabi, K. (2016) Adherence to ICT Security and Privacy Policies in Saudi Arabia. *International Journal of Computer Applications*, **147**, 13-18. https://doi.org/10.5120/ijca2016910974

[3] Appenzeller, T. (2004) The End of Cheap Oil. *National Geographic*, **205**, 80-109.

[4] Alassafi, M.O., Alharthi, A., Walters, R.J. and Wills, G.B. (2017) A Framework for Critical Security Factors That Influence the Decision of Cloud Adoption by Saudi Government Agencies. *Telematics and Informatics*, **34**, 996-1010. https://doi.org/10.1016/j.tele.2017.04.010

[5] Bawazir, S.A. (2006) The Key Factors of Successful Sustainable Development: E-Government in Saudi Arabia as an Example. Proceedings of the Saudi 6*th National Computer Conference*, 13-18. http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033484.pdf

[6] Geller, J., Ae Chun, S. and Wali, A. (2014) A Hybrid Approach to Developing a Cyber Security Ontology. Proceedings of 3*rd International Conference on Data Management Technologies and Applications*, **1**, 377-384. https://doi.org/10.5220/0005111503770384

[7] Ahmed, S., Buragga, K. and Ramani, A.K. (2011) Security Issues Concern for E-Learning by Saudi universities. 2011 13*th International Conference on Advanced Communication Technology*, Gangwon-Do, 13-16 February 2011, 1579-1582.

[8] Elmogazy, H. and Bamasak, O. (2013) Towards Healthcare Data Security in Cloud Computing. 2013 8*th International Conference for Internet Technology and Secured Transactions*, London, 9-12 December 2013, 363-368.

[9] Othman, S.B., Trad, A., Youssef, H. and Alzaid, H. (2013) Secure Data Aggregation in Wireless Sensor Networks. 12*th Annual Mediterranean Ad Hoc Networking Workshop*, Ajaccio, 24-26 June 2013, 55-58. https://doi.org/10.1109/MedHocNet.2013.6767410

[10] Rahman, S.M.M. (2014) Towards Integrity Protection of Software for E-Health Data. 2014 *IEEE International Conference on Multimedia and Expo Workshops*, Chengdu, 14-18 July 2014, 1-5.

[11] Baig, O., Ai-Harthi, Y.S. and Al-Tubaishi, E. (2014) Game-Theoretic Algorithm Stimulating Cooperation in Multi-Hop Wireless Networks. 5*th International Conference on Game Theory for Networks* (GAMENETS), Beijing, 25-27 November 2014, 1-5. https://doi.org/10.1109/GAMENETS.2014.7043691

[12] Zeb, K., Baig, O. and Asif, M.K. (2015) DDoS Attacks and Countermeasures in Cyberspace. 2*nd World Symposium on Web Applications and Networking*, Hammamet, 21-23 March 2015, 1-6.

[13] Faisal, M. and Mathkoor, H. (2015) SDTP: Secure Data Transmission Protocol in Ad Hoc Networks Based on Link-Disjoint Multipath Routing. 2*nd World Symposium on Web Applications and Networking*, Hammamet, 21-23 March 2015, 1-5. https://doi.org/10.1109/WSWAN.2015.7210348

[14] Kurniawan, F., Khalil, M.S., Khan, M.K. and Alginahi, Y.M. (2013) Exploiting Digital Watermarking to Preserve Integrity of the Digital Holy Quran Images. *Taibah University International Conference on Advances in Information Technology for the Holy Quran and Its Sciences*, Al-Madinah, 22-25 December 2013, 30-36.

[15] Alsmadi, I.M. (2013) Techniques to Preserve the Integrity of the Electronic Versions of the Nobel Quran. *Taibah University International Conference on Advances in Information Technology for the Holy Quran and Its Sciences*, Al-Madinah, 22-25 December 2013, 52-56.

[16] Munir, K. (2015) Security Model for Cloud Database as a Service (DBaaS). *International Conference on Cloud Technologies and Applications*, 1-5. https://doi.org/10.1109/CloudTech.2015.7336974

[17] Abuhaija, B., Awadelkarim, A.M., Shilbayeh, N. and Alwakeel, M. (2014) A Model for Securing Islamic Websites: Formal Specification Paradigm: IT Research Center for the Holy Quran and Its Sciences (NOOR). 4*th International Conference on Artificial Intelligence with Applications in Engineering and Technology*, Madinah, 80-85.

[18] Ahmad, A., Nasser, N. and Anan, M. (2016) An Identification and Prevention of Theft-of-Service Attack on Cloud Computing. *International Conference on Selected Topics in Mobile & Wireless Networking*, Cairo, 11-13 April 2016, 1-6. https://doi.org/10.1109/MoWNet.2016.7496632

[19] Alghamdi, A., Alshamrani, M., Alqahtani, A., Al Ghamdi, S.S.A. and Harrathi, R. (2016) Secure Data Aggregation Scheme in Wireless Sensor Networks for IoT. *International Symposium on Networks*, *Computers and Communications*, Hammamet, 11-13 May 2016, 1-5. https://doi.org/10.1109/ISNCC.2016.7746071

[20] Alkanhel, R. and Ambroze, M.A. (2016) Extended Grouping of RFID Tags Based on Progressive Edge-Growth Methods. 5*th International Conference on Electronic Devices*, *Systems and Applications*, Ras Al Khaimah, 6-8 December 2016, 1-5. https://doi.org/10.1109/ICEDSA.2016.7818544

[21] Kuppuswamy, P., Banu, R. and Rekha, N. (2017) Preventing and Securing Data from Cyber Crime Using New Authentication Method Based on Block Cipher Scheme. 2*nd International Conference on Anti-Cyber Crimes*, Abha, 26-27 March 2017, 113-117. https://doi.org/10.1109/Anti-Cybercrime.2017.7905274

[22] Dhaou, I.B., Gia, T.N., Liljeberg, P. and Tenhunen, H. (2017) Low-Latency Hardware Architecture for Cipher-Based Message Authentication Code. *IEEE International Symposium on Circuits and Systems*, Baltimore, 28-31 May 2017, 1-4.

[23] Zheng, Q., Wang, X., Khan, M.K., Zhang, W., Gupta, B.B. and Guo, W. (2018) A Lightweight Authenticated Encryption Scheme Based on Chaotic SCML for Railway Cloud Service. *IEEE Access*, **6**, 711-722. https://doi.org/10.1109/ACCESS.2017.2775038

[24] Elleuchi, M., Boujeleben, M., Abid, M. and BenSaleh, M.S. (2017) Securing RPL-Based Internet of Things Applied for Water Pipeline Monitoring. 25*th International Conference on Software*, *Telecommunications and Computer Networks*, Split, 21-23 September 2017, 1-7. https://doi.org/10.23919/SOFTCOM.2017.8115580

[25] Shuaibu, M.B. and Ibrahim, R.A. (2017) Web Application Development Model with

Security Concern in the Entire Life-Cycle. 4*th IEEE International Conference on Engineering Technologies and Applied Sciences*, Salmabad, 29 November-1 December 2017, 1-6. https://doi.org/10.1109/ICETAS.2017.8277849

[26] Kurdi, R., Hersi, F., Bahagari, S., Kaosar, M., Qaisar, S.M. and Subasi, A. (2017) A Mobile Fingerprint Authentication in Saudi Arabian Call Centers. *International Conference on Electrical and Computing Technologies and Applications*, Ras Al Khaimah, 21-23 November 2017, 1-4. https://doi.org/10.1109/ICECTA.2017.8252000

[27] Communications and Information Technology Commission (2011) Information Security Policies and Procedures Development Framework for Government Agencies. KSA Communications and Information Technology Commission. http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf

[28] Thakur, K., Ali, M.L., Gai, K. and Qiu, M. (2016) Information Security Policy for E-Commerce in Saudi Arabia. 2*nd IEEE International Conference on Big Data Security on Cloud*, New York, 9-10 April 2016, 187-190. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.14

[29] Razek, N.A. (2014) Academic Integrity: A Saudi Student Perspective. *Academy of Educational Leadership Journal*, **18**, 143. https://ecommons.udayton.edu/edc_fac_pub/3/

[30] Sheikh, A.A. (2017) Cyber Security Framework for Saudi Arabian Monetary Authority. 1-56. http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

[31] Madini, O.A., Alharthi, A., Walters, R.J. and Wills, G.B. (2016) Security Risk Factors That Influence Cloud Computing Adoption in Saudi Arabia Government Agencies. *International Conference on Information Society*, Dublin, 10-13 October 2016, Vol. 1, 1-4.

[32] Aldossary, A.A. and Zeki, A.M. (2013) The Influence of Students' Knowledge on Security towards Their Behavior with Security Risks within the Context of Saudi Arabia. *International Conference on Advanced Computer Science Applications and Technologies*, Kuching, 23-24 December 2013, 1-4. https://doi.org/10.1109/ACSAT.2013.9

[33] Gruber, T.R. (1993) A Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition*, **5**, 199-220. https://doi.org/10.1006/knac.1993.1008

[34] McGuinness, D.L. and Van Harmelen, F. (2004) OWL Web Ontology Language Overview. *W3C Recommendation*, **10**, 2004. http://www.w3.org/TR/2004/REC-owl-features-20040210/