Addis Ababa University (Since 1950)

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCES

APPLICATION OF CASE BASED REASONING SYSTEM FOR IDENTIFYING INSIDERS THREAT BEHAVIOR IN TELECOM: THE CASE OF ETHIO TELECOM

YOHANES HALEFOM

JUNE 2019

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCES

APPLICATION OF CASE BASED REASONING SYSTEM FOR IDENTIFYING INSIDERS THREAT BEHAVIOR IN TELECOM: THE CASE OF ETHIO TELECOM

A THESIS SUBMITTED TO THE SCHOOL OF INFORMATION SCIENCES OF ADDIS ABABA UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEM

YOHANES HALEFOM

JUNE 2019

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCES

APPLICATION OF CASE BASED REASONING SYSTEM FOR IDENTIFYING INSIDERS THREAT BEHAVIOR IN TELECOM: THE CASE OF ETHIO TELECOM

NAME AND SIGNATURE OF MEMBERS OF THE EXAMINING BOARD

ADVISOR	**SIGNATURE**
MILLION MESHESHA (PhD)	
EXAMINER	**SIGNATURE**
TEMTIM ASSEFA (PhD)	
EXAMINER	**SIGNATURE**
MELKAMU BEYENE (PhD)	

YOHANES HALEFOM

JUNE 2019

ACKNOWLEDGEMENT

Thanks **God**, the merciful and the passionate, for providing me the opportunity to step in the excellent world of science. To be able to step strong and smooth in this way, I have also been supported and supervised by many people to whom I would like to express my deepest gratitude below.

Foremost, I would like to express my sincere gratitude to my advisor **Dr. Million Meshesha** for the continuous support of my research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have Imagined having a better advisor and mentor for my study.

Then, in order to this thesis research work come true, though words are not strong enough to express my feeling and thanks giving, my sincere thanks goes to **Mr. Yohannes Tilahun**, my immediate supervisor for your understanding and guidance whenever the load on thesis work impacted the work, and you were the first persons whom imparted my burdens. Thank You.

I gratefully acknowledge the contributions of **Mr. Getinet Wondmeneh** who was instrumental in the overall work. His expertise in building information modelling and his commitment towards the work was a significant influence in shaping many of the concepts presented in this thesis. I would like to thank my friend and colleague **Benat Mohammedamin** for her frequent help and support.

Last but not the least, I would like to thank my family: my parents **Askalech Yimer** and **Halefom Abadi**, for giving birth to me at the first place and supporting me spiritually throughout my life.

List of Tables

List of Figures

List of Acronyms

CBR – Case Based Reasoning

DDoS - Distributed Denial of Service

FDRE – Federal Democratic Republic of Ethiopia

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

ISDR - Information Systems Design Research

jCOLIBRI- Java Class Ontology Libraries Integration for Building Reasoning Infrastructure

KBS – Knowledge based system

SPSS - Statistical Package for the Social Sciences

Contents

Abstract

On this research work the researcher has made an attempt on applying case-based reasoning system in depicting employee's behavior towards potential frauds to be committed by identifying at risk employees and recommending possible related fraud types to be committed, by using human observable behaviors. The required knowledge was acquired from two group of experts, seven previously investigated insider cases, document analysis and other relevant information through a six-point Likert scale questionnaire survey. Investigated cases were gathered from Ethio telecom legal department and information science department. The domain experts were selected from Addis Ababa University, FDRE attorney general and self-employed personnel, using purposive sampling.

For modeling purpose of the acquired knowledge, hierarchical tree modeling technique were used. Attributes that are relevant and have direct impact on the decision were selected and the case structure formulated.

The prototype is developed using the Object-Oriented framework JCOLIBRI1.1. The system has the capability in retrieving, reusing, revising, and retaining new cases. And here nearest neighbor retrieval algorithm was used while the system retrieves cases from the knowledge base. In order to assure the CBR system has meet the requirement needed, evaluation was conducted on both the system performance and user acceptance test.

The overall evaluation result shows that the case-based reasoning prototype for insider threat mitigation is very encouraging as the retrieval performance of the prototype registers an average value of 82.14% precision and 82.85 % recall with average accuracy of 94.90%. And also, the system has registered an average grade of "very good" in user satisfaction test result.

Generally, the work has achieved its objective by developing the expected prototype with an encouraging system performance and user acceptance test result on designing knowledge-based system for insider threat mitigation using human observable behaviors.

CHAPTER ONE

Introduction

1.1 Background

Telecommunications reach deep into the daily circumstances of individuals, businesses, and governments. Telecoms, in fact, touches nearly everything and everyone, and, along with energy, forms a foundation upon which all other critical infrastructure operates. Due to the breadth and depth of services offered by telecom companies, there is a significantly increased risk of cyber security threats. While the telecom industry is more equipped to protect its networks due to the nature of the industry, various progressive threats exist which need to be mitigated. Some of these attacks could lead to denial of service, protecting these networks from attacks is thus an important aspect that cannot be ignored. According to PwC's Global State of Information Security, (2016), IT security incidents in the telecoms sector increased by 45% in 2015 compared to the year before. Telecoms providers need to arm themselves against this growing risk.

Insider threats can be divided into seven sub-categories, based on the manner in which they affect the organization's information security goals, and the human factors which lead an insider to act in a malicious manner. We can also name the insider threat categories in term of the impact and the actions that the insider uses to achieve his aims. These are: a) insider IT sabotage, b) insider IT fraud, c) insider theft of intellectual property, d) insider social engineering, e) unintentional insider threat incident, f) insider in cloud computing, and g) insider national security (D. Cappelli, A. P. Moore, and R. Trzeciak 2010). However, organizations could be affected by more than one category of malicious insider threat at the same time. The researcher has contacted the IT strategy Officer at Ethio telecom, and the response shows that there are many investigated cases that cause many loses to the company, which are committed by insiders. They also noted that there is an illegal internal cyber security activity in almost all products and assets of the company. The corporate communications managers at Ethio telecom officially announces that Ethiopia loses over 52 million dollars by telecom fraud in the year 2016/17.

1.1. 1 Insiders and insider threats

The term 'insiders' is broad, could cover a spectrum of users, and has no evident definition. But according to several authors (Ophoff et al., 2014; Hunker & Probst, 2011; Costa et al., 2005; Chinchani et al., 2005), insiders are legitimate users, familiar with internal systems and could be aware of organization's security countermeasures. Hamin (2000) and Silowash (2012) also consider employees, and consultants, and stakeholders as insiders. Greitzer (2014) and Colwill (2009) divide insiders into two categories: malicious (intentional) insiders and unintentional insiders. Ophoff et al. (2014) add a third category, 'motives', to the previous categories, for describing behaviors that could be considered abnormal, but do not lead to security incidents.

Insider threats mainly refer to the intent of dishonest employees to commit some form of cyber-crime Dhillon (2001). Insiders are capable of disrupting operations, corrupting data, infiltrating sensitive information, or generally compromising an IT system, thereby causing loss or damage (Cappelli, 2009; Cummings 2012). As the discussion on the insider threat has evolved considerably over the past decade, so has the very definition of the term 'insider'. Nowadays, it is not only employees who have privileged access to the assets of an organization, but also volunteers, consultants and contractors (Brancik, 2007). Access is also given to business partners or fellow members of a strategic alliance, whereas contractors now include employees of a cloud service provider. Hence, a more appropriate alternative to the term 'insider' would be a '(person with) specialized access' (Hartel, 2010). Misusing or abusing company assets by individuals, who possess permissions and have knowledge about company internal systems, has significantly increased in recent times (Legg et al., 2013), therefore this issue is considered the second greatest cybersecurity threat (Greitzer et al., 2009). These threats have serious consequences, and some have become more intelligent and sophisticated (Legg et al., 2013). However, the main concern of the vast majority of companies and organizations is to protect themselves from external attacks, and they are largely either overlooking or oversimplifying potential internal threats, thus they do not plant countermeasures that can reduce these threats perpetrated by insiders (Grant, 2009). Consequently, traditional protection solutions for external attacks are unable to detect insider threats.

As the insider-threat problem has grown, it has also received great attention within the research community. There have been in-depth discourses on everything from what exactly an insider threat is and what the range of human and psychological factors involved are, to how threats can be predicted, detected and effectively addressed with appreciation of technological and behavioral advances and theories. These approaches have resulted in numerous models and frameworks for insider threat, each with its distinct perspective on the problem and specific area which it aims to address. In spite of these advances in research and the various proposals, however, there is arguably still no unifying framework which seeks to fully characterize the insider-threat problem space. That is, defining which insiders attack, why they attack, the human factors that lead to accidental threats, how one's background may impact likelihood of attack, what behavior may be exhibited before or during an attack, what the common attack vectors and steps within an attack are, and what assets and vulnerabilities are typically targeted.

The focus of this study is therefore to address this gap and present a CBR system for understanding and characterizing insider threat behavior that is grounded in real-world threat data and pertinent literature. The researcher tries to draw on insider-threat cases from Ethio-telecom, broad survey data and existing research, to understand and categorize the threats.

1.1.2 Case-based Reasoning

Case-based reasoning (CBR) is a problem-solving approach that makes use of previous, similar situations and reuses information and knowledge about such situations (Kolodner, 1993). Basically, CBR technology is a reasoning procedure or framework instead of a specific algorithm (Watson, 1999). It uses different technologies and algorithms to solve problems.

CBR is a problem-solving paradigm that in many respects is fundamentally different from other major AI approaches (Aamodt & Plaza, 1994). CBR, instead of relying solely on general knowledge about a problem domain, or making associations along generalized relationships between problem descriptors and conclusions, it can utilize the specific knowledge of previously experienced, concrete problem situations. A new problem is solved by finding a similar past case, and reusing it in the new problem situation. A second important difference is that CBR has also been an approach to be incremental, sustained learning, since a new experience is retained each time a problem has been solved, making it immediately available for future problems. The CBR

field grew rapidly over the last few years, as seen by its increased share of papers at major conferences, available commercial tools, and successful applications in daily use.

1.2 Motivation

Current practice in insider threat detection tends to be reactive as it focuses on detecting malicious acts after they occur with the aim of identifying and disciplining the perpetrator. Typical approaches incorporate forensic measures including external threat/defense-oriented appliances such as Intrusion Detection or Prevention Systems (IDS/IPS). The majority of Chief Security Officers (CSOs) focus only on employing technologies to protect from external threats, and do not implement necessary countermeasures against insiders (Grant, 2009). This fact can be clearly deduced through the scarcity in the policies, procedures and mitigation solutions that control employees' bad behavior. Insider Threats are not a technology Problem. Insiders are people, not computers. Treating insiders as a technology problem ignores the human aspects of motivation and behavior. Detecting insiders requires a defined process and a focused team in addition to detection technologies. Even those detecting technologies are managed by humans. So, it will be better on giving attention for Employees behavior.

The consequences of insider threats are unlimited, and could be tangible or intangible, but they could be generalized to financial loss and damage of reputation of the organization (Ophoff et al., 2014).

Cappelli et al. (2004) describe 15 financial loss cases between 1996 and 2002 in the financial sector. They also mention that the financial gain is the most prevalent motive throughout the 26 incidents examined, and show that preforming internal fraud activities does not require high technical skills. There are other impacts, such as business disruption and customer loss, but they could fall under category of financial loss. However, undoubtedly any publicly disclosed insider threat incident could indirectly lead to damage of reputation, thus loss of reputation would be considered the ultimate result of any insider attack if publicly disclosed.

Burroughs and James (2005) review personality research to identify individual differences that may account for counterproductive work behavior. People with certain dispositions are found more likely to engage in antisocial behaviors or to direct harmful actions against others. This may include exhibiting traditional workplace retaliation behaviors in order to right a wrong, in response to organizational upheaval or organizational injustice, and in response to breach of contract (e.g., psychological contract breach) (Ambrose, et al., 2002; Folger and Skarlicki, 2005; Pearson and

Anderson, 2005; Rosen, Chang, Johnson and Levy, 2009; Tripp and Bies, 2009). Shropshire (2009) recently conducted a canonical analysis of sixty-two intentional security breaches by insiders. His study indicated a positive correlation between four general variables (Financial changes, relationship strains, substance abuse, and job changes) and predictions of insider threat, each of which is observable by conscientious managers and/or supervisors. The research conducted by Verizon and the U.S. Secret Service (2010), Cappelli, Moore, Trzeciak and Shimeall (2009), and the NIAC (2008) assessed the relationship between insiders' backgrounds and motivations and their resulting deviant behaviors. Despite a growing body of research into the psychology and motivation of insiders, it is difficult to predict who will commit security fraud (Kramer, Heuer and Crawford, 2005). Shaw and Fischer (2005) noted that most of the threats in their study could have been prevented by timely and effective action to address the anger, pain, anxiety, or psychological impairment of perpetrators, who exhibited signs of vulnerability or risk well in advance of the crime.

1.3 Statement of the Problem

As Ethio telecom is the only telecom service provider in the country, it operates and manage the countries' networks, voice and data transmissions and store vast amounts of sensitive data, and this makes them a highly attractive target for cybercriminals in search of financial gain, nation-state sponsored actors launching targeted attacks. Even if the cases related with insider threats are not officially released, the researcher have observed so many internal fraud activities on different departments of the company, which are investigated by the company's IS department.

As the insider-threat problem has grown, so too has the attention it has received within the research community.

There have been in-depth discourses on everything from what exactly an insider threat is (J. Hunker and Probst,2011 and what the range of human and psychological factors involved are (Colwill,2009), to how threats can be predicted, detected and effectively addressed with appreciation of technological and behavioral advances and theories. These approaches have resulted in numerous models and frameworks for insider threat, each with its distinct perspective on the problem and specific area which it aims to address. In spite of these advances in research and the various proposals, however, there is arguably still no unifying framework which seeks to fully characterize the insider-threat problem space. That is, defining which insiders attack, why

they attack, the human factors that lead to accidental threats, how one's background may impact likelihood of attack, what behavior may be exhibited before or during an attack, what the common attack vectors and steps within an attack are, and what assets and vulnerabilities are typically targeted.

New technologies need to be utilized to support security professionals in the security control process to assist the daily activities of problem solving and decisions making of the cases. These require organizing knowledge of security professionals and documents, both tacit and explicit knowledge.

Reasoning by reusing past cases is a powerful and frequently applied way to solve problems for humans. This claim is also supported by results from cognitive psychology research. Part of the foundation for the case-based approach is its psychological plausibility. Several studies have given empirical evidence for the dominating role of specific, previously experienced situations (what we call cases) in human problem solving (Ross, 1989).

Therefore, the aim of this study is to design prototype, case-based reasoning in knowledge-based system that advises in the identification and controlling insider threat's behavior. Which is grounded in real-world threat data and pertinent literature. The researcher draws on insider threat cases from Ethio-telecom and broad survey data and existing research.

Therefore, this study investigates and answer the following questions.

- What type of knowledge is required to design a CBR system which can assist experts in insider threat behavior identification and control?
- What is the appropriate modelling and inferencing techniques to implement the CBR for insider threat behavior identification?
- To what extent the prototype performs in detecting insider threats.

1.4 Objective of the study

1.4.1 General objective

The main objective of this study is to design and develop a prototype CBR system that enables to identify insiders threat behavior in telecom.

1.4.2 Specific Objectives

- To review literature on related research works in order to have an understanding on concepts, principles and technologies of knowledge-based system.
- To extract the domain knowledge which is used in identification of employee's behavior from experts and available literature.
- To analyze and model the domain knowledge and construct structured domain knowledge to gain new knowledge.
- To build a prototype CBR system for depicting employee's behavior towards potential frauds to be committed.
- To test and evaluate the performance of the prototype system.

1.5 Scope and limitation

The scope of this research is limited to the retrieval of the most similar cases comparing the case at hand to the library of past investigated-cases, using the CBR approach. The cases to be considered in this research are those investigated and closed cases by Ethio-telecom Information security and legal department. The study is intended to develop and evaluate CBR prototype system for depicting employee's behavior towards potential frauds to be committed, and giving advisory services primarily for the domain experts, human resource managers and then for any interested party. Cyber Security Threats facing telecommunications companies include; Distributed Denial of Service (DDoS) attacks, targeted attacks; poorly configured access controls, inadequate security for 2G/3G communications, the exploitation of vulnerabilities in network and consumer devices, and Insider threats. However, the study covered only insider threats, and on identifying their observable behaviors, then finally depicting those behaviors before potential frauds are committed.

The study is limited to develop a prototype knowledge-based system for the purpose of identifying insider threats behavior, and doesn't give punishment decision for the new cases.

1.6 Significance of the study

The study helps in reducing insider threats facing the company, giving advisory services while identifying and understanding insider threat's behavior, for screening employees while internal job transfer takes place, and to take the necessary action before the threat takes place. It also encourages Ethio telecom senior officials to focus on insider threats behavior in the processes of controlling insider threat. The prototype has great significance to teach primary security professionals, general reactionaries and the company's higher management in order to have well understanding about insiders' behavior. The developed prototype CBR system can be used to give advising services on identifying and understanding insider threat's behavior happening, in order to enable to take the possible preventing and control action. Employees that engaged themselves on fraudulent activities will be alarmed before more serious things are happening to them, so that they will stop their illegal activities. Customers of Ethio telecom also will have better satisfaction, increase their reliability on privacy issues and inconveniences, and will have better reliance on the company services provided by the employees. This research can serve as a base for future researchers interested on this area. This study also initiates other organizations to turn their face to intelligence-based insider's identification mechanism.

1.7 Methodology

The study follows design science research approach for the overall work of this study. The researchers, on the next sections has discussed What, How, and Why is each step of the research process done in detail. The fundamental principle of design science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. (Alan Hevner, 2010).

CHAPTER TWO

LITERATURE REVIEW

2.1 Background of Ethio telecom

As a continuation of the 2005/06 – 2009/10 five-year plan and after concentrating its efforts on education, health and agriculture, the Ethiopian government has decided to focus on the improvement of telecommunication services, considering them as a key lever in the development

of Ethiopia. Ethio telecom is born, on 29th November 2010, from this ambition of supporting the steady growth of our country, within the Growth and Transformation Plan (GTP), with ambitious objectives for the year 2015. The Ethiopian government has decided to transform the telecommunication infrastructure and services to world class standard, considering them as a key lever in the development of Ethiopia. Thus, Ethio telecom is born from this ambition to bring about a paradigm shift in the development of the telecom sector to support the steady growth of our country.

2.2 Overview

AI is one of the newest fields in science and engineering. Work started in earnest soon after World War II, and the name itself was coined in 1956. Along with molecular biology, AI is regularly cited as the "field I would most like to be in" by scientists in other disciplines. A student in physics might reasonably feel that all the good ideas have already been taken by Galileo, Newton, Einstein, and the rest. AI, on the other hand, still has openings for several full-time Einsteins and Edisons. AI currently encompasses a huge variety of subfields, ranging from the general (learning and perception) to the specific, such as playing chess, proving mathematical theorems, writing poetry, driving a car on a crowded street, and diagnosing diseases. AI is relevant to any intellectual task; it is truly a universal field (Russell, Stuart and Norvig, Peter, 2009).

Artificial intelligence is the science of transforming human intelligence into programs that enable computers to make educated (intelligent) decisions and choices. It is a technique where in non-living entities transform and link simple elements of information to form complex functions and interrelationships. Expert or knowledge-based systems (KBS) are one of such AI techniques (Watson and Marir,1994).

Below in figure 2 we can see eight definitions of Artificial Inelegant defined by different scholars at different time. The definitions on top are concerned with thought processes and reasoning, whereas the ones on the bottom address behavior. The definitions on the left measure success in terms of fidelity to human performance, whereas RATIONALITY the ones on the right measure against an ideal performance measure, called rationality. A system is rational if it does the "right thing," given what it knows. Historically, all four approaches to AI have been followed, each by different people with different methods. A human-centered approach must be in part an empirical science, involving observations and hypotheses about human behavior. A rationalist1 approach

involves a combination of mathematics and engineering. The various group have both disparaged and helped each other (Russell, Stuart and Norvig, Peter, 2009).

Thinking Humanly Thinking Rationally	**Thinking Rationally**
"The exciting new effort to make computers think . . . machines with minds, in the full and literal sense." (Haugeland, 1985) "[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning . . ." (Bellman, 1978)	The study of mental faculties through the use of computational models." Charniak and McDermott, 1985). "The study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)
Acting Humanly	**Acting Rationally**
"The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990). "The study of how to make computers do things at which, at the moment, people are better." (Rich and Knight, 1991)	"Computational Intelligence is the study of the design of intelligent agents." (Poole et al., 1998). "AI . . . is concerned with intelligent behavior in artifacts." (Nilsson, 1998)

Figure 1Some definitions of artificial intelligence, organized into four categories. Adopted from (Russell, Stuart and Norvig, Peter, 2009).

2.2 Knowledge based systems

KBS incorporates knowledge that is symbolic, not only symbolic as well as numeric. It reasons with judgmental, imprecise, and qualitative knowledge as well as with formal knowledge of established theories. Its knowledge is simply and explicitly represented in terms familiar to specialists, and is separate from its inference procedures. It provides explanations of its line of reasoning and answers to queries about its knowledge. It is incrementally refinable and extensible. More details can be specified to refine its performance; more concepts and links among concepts can be specified to broaden its range of applicability, and It is an expert system if it provides expert-level solutions (Reid, 1985).

Expert or knowledge-based systems (KBS) are one of the success stories of Artificial Intelligence (AI) research. In a recent survey the UK Department of Trade & Industry found over 2000 KBS

in commercial operation (the survey excluded KBS in University research laboratories) (DTI, 1992).

2.3 Case Based Reasoning

As a significant branch of Artificial Intelligence (AI), Case-Based Reasoning (CBR) has received more and more research attention. In the last few decades, CBR has grown from a quite new area to a subject of major influence. Much work has been dedicated to this topic, including its basic principle, methodologies and applications (Reisbeck and Schank 2009). CBR systems have also been used to solve a wide range of problems. Examples of the applications of the CBR systems include medical diagnosis, time series prediction, product design and planning etc. The basic idea behind CBR is that reasoning and problem-solving are based on the most specific experiences available instead of general abstract knowledge or rules. In this way, case-based reasoning provides a new method for building intelligent systems (Kolodner,1993).

2.3.1 CBR History and Development

Case Based Reasoning (CBR) is commonly interpreted as reasoning through remembering. This method adapts previously known successful solutions to new similar problems. The advantage of CBR over other AI techniques lies in the fact that an explicit domain model is not necessary; data/information extraction is limited to gathering case histories. CBR implementation is based on identifying significant features that describe a case, contrary to the development of an explicit model. It is a technique of machine learning through knowledge acquisition for problem solving and interpretation. Utilizing the advantages of databases to store cases, CBR tools can handle large volumes of data with ease. Learning is simply performed by acquiring new successful cases for the database. Hence maintenance and enhancement of the CBR model can be performed with greater ease.

Watson and Marir,1994; Aamodt and Plaza,1994 has tried to review the history of CBR, its development and the role of cases and the researcher has summarized it as below. They proposed a conceptual memory structure called scripts containing information about stereotypical events similar to human general knowledge which allow us to set expectations and perform inferences. The role of cases i.e. the memory of previous situations and situation patterns (termed as memory organization packets - MOPs with respect to learning and problem solving was explored by Roger

Schank in 1984. Work on transformational and derivational analogy which developed the mapping, adaptation and replay process for CBR was performed by Carbonell (1983 – 1986). Roger Schank's work at Yale University in early eighties produced an intelligent model for CBR and the first CBR applications based on this mode l. The first complete CBR system 'CYRUS' was developed by Janet Kolodner. Current CBR work can be divided into two categories: CBR research and applied CBR **(Leake, 1995).**CBR research is the study of algorithms and knowledge needed to enhance understanding of human reasoning and/or the scientific understanding of the CBR process itself. Applied CBR applies and builds upon existing CBR theories in a variety of domains sometimes using the aid of other related reasoning methods to achieve the desired goal.

Case based reasoning is an inherent reasoning methodology utilized by all humans in various facets of life. "In real life, when we are having difficulty with a task or a situation, we tend to seek advice from someone who might know about the problem at hand. If this someone does know the answer, we not only benefit directly from what they tell us, we acquire a new case. Because our problems are usually not so clear cut, and answers are not so directly applicable, this process is not as simple as it sounds. We might discuss our problem with someone who is not exactly an expert but can offer good advice. They might respond with a story from their own lives, and if the story is well-told and seems germane to our problem, we will take the added step of adapting it to make it relevant to our own lives" **(McGarry, 2006).** Reasoning by re-using past experiences or cases is a technique frequently applied by humans to solve problems. Results of cognitive psychological research support similar conclusions.

Key issues in applying CBR methodology lie in **(Leake, 1995):**

1. Situation assessment/retrieval: procedure to be followed to retrieve the most relevant prior cases.

2. Case application and evaluation: Investigation of which retrieved case / cases would be most relevant and how the retrieved case(s) methodology or solution will apply to the new case, as well as, how effectively will it apply.

3. Case adaptation: Modifying the chosen case's solution to fit the problem case.

4. Storage: When and how to save the problem case and modified solution for future reuse.

In CBR application there are two types of case categories:

1. A previous experience or situation which has been obtained, studied and learned from, so that it can be applied to solve new problems is known as a past case, previous case, stored case, or retained case.

2. A new problem to be solved is described as an unsolved case or new case. The formal definition of a case is: "A case is a contextualized piece of knowledge representing an experience. It contains the past lesson that is the content of the case and the context in which the lesson can be used. Typically, a case comprises:

1. The problem that describes state of the world when the problem occurred.

2. The solution which states the derived solution to that problem, and/or

3. The outcome which describes the state of the world after the case occurred" **(Watson and Marir ,1994).**

CBR systems learning takes place in two phases. CBR system learns new cases from a successful solution, and from problems and recovery methods in failed solutions. This enables the system to constantly and automatically refine its knowledge. Despite the fact that CBR in the raw form merely searches for cases it differs from database searches as it is capable of performing partial matches and adaptation of partial matches to fit the problem case despite the lack of complete domain knowledge. This gives CBR its' robustness and flexibility **(Leake, 1995).**

2.3.2 Case Based Reasoning Procedure

The CBR procedure as reviewed in **(Aamodt and Plaza,1994; Leake, 1995)** is summarized. The CBR technique utilizes continuous and constant learning as each new experience is stored each time a problem is solved, making it instantly available for the next problem. In an ideal CBR approach, if a problem is successfully solved it can be directly stored for future use. If a failure occurs, the reason for failure is evaluated and determined. This is then stored in order to avoid the same mistake in the future.

A CBR model can utilize a variety of different methods for ordering, retrieving, using and indexing the knowledge stored in previous known cases. Cases can be maintained as individually identifiable experiences and stored as separate knowledge units or can be maintained as generalized cases by grouping similar cases and stored by splitting up into subunits within the

knowledge structure. These stored cases are then indexed in different ways for organizational and retrieval purposes. The solution of a retrieved case can be used directly for the problem case or modified according to the differences between the retrieved and problem cases. This process of case retrieval through matching, adaptation of retrieved case solution and learning from an encounter could be based upon a deep model of general domain knowledge or a shallow model of detail knowledge or may be according to an apparent syntactic similarity. The CBR model may function with or without user intervention and interaction. The case base used by CBR may contain a many widely distributed cases or limited quantity of typical cases. This general approach of CBR is used in variants of Case Based Reasoning such as exemplar-based reasoning, memory-based reasoning etc. **(Aamodt and Plaza,1994; Leake, 1995).**

In exemplar-based reasoning cases are categorized into classes and each class has a generalized solution. The set of classes forms the set of possible solutions. This method is essentially based upon finding the right class for the new problem, i.e. a problem of classification. Once the class is identified, the solution of the class forms the solution of the problem case. Hence, this method does not entail modification of the found solution. Instance-based reasoning is a specialization of exemplar-based reasoning as it applies a non-generalization-based approach developing a highly syntactic CBR-approach. To offset the lack of guidance from general background knowledge a relatively large number of cases is required in order to approach a concept definition. [1, 18] Memory-based reasoning considers reasoning to be centralized on a process of accessing and searching a large collection of cases in memory. Hence, the way memory is organized and searched forms a large part of this technique. Parallel processing is a technique utilized by this method for rapid searching **(Aamodt and Plaza,1994; Leake, 1995).**

Case-based reasoning assumes that each case stored has a certain amount of richness of information in it, as well as a certain degree of complexity to it. This technique is able to adapt a retrieved solution to suit the given problem case within the same domain, utilizing a variable amount of general background knowledge **(Aamodt and Plaza,1994; Leake, 1995).** Analogy-based reasoning is a technique similar to case-based reasoning which is applied across domains. The main focus of research is to identify and apply techniques to perform matching and adaptation of cases across domains **(Aamodt and Plaza,1994; Leake, 1995).** All variants of CBR involve search and retrieval of cases from storage. To perform this, efficient indexing of stored cases is

required. In general, indexing should be predictive so as to give an indication of the key parameters of the case and what the case is used for. It should be sufficiently abstract and concrete to permit domain expansion for future use of the case-base. Automated as well as manual processes have been utilized for indexing. Manual indexing requires identifying how the case would be used and under what conditions would it be useful keeping in mind the requirements of the reasoner. Common belief is that people tend to be better at choosing indices than automated algorithms. Automated indexing techniques include checklist-based indexing, difference-based indexing, similarity and explanation-based indexing (Aamodt and Plaza,1994; Leake, 1995).

Similarity and explanation-based method; group cases based on their similarity and then create indices for the cases based on the features that the cases don't share with their group **(Watson and Marir,1994).** The CBR application CHEF for example uses explanation and similarity-based indexing to group recipe cases (**Hammond,1989**). Similarity in the properties of a particular entity for examples strawberries and apples are used to classify it under the category 'fruit'. Explanations are used to identify definitive reasons for failure of a particular case in such a way that it can be generalized and applied. For example, if fruit is juicy and an 'x' amount of leavening agent is to be used in the recipe for cake, the recipe will fail because the fruit will release water. To prevent water an 'x + y' amount of leaving agent should be used. Hence, the index can contain "recipe is of type cake and dish is juicy fruit" (Kolodner, 1993).

2.3.3 Knowledge Representation

The cases for CBR should be stored in a structure that considers the indices that characterize the case as well depict what the cases represent. The structure should be able to provide efficient search retrieval and addition mechanisms as well as "preserve the semantic richness of the case". These structures are called as case memory models, which are divided into two basic types, dynamic memory model and category-exemplar model (Watson and Marir,1994).

Dynamic memory model is composed of basic units of dynamic memory called Memory Organization Packets (MOP's) which are of two types: (a) instances which denote cases, events or objects and (b) abstractions which are generalized versions of instances called. The case memory then forms a hierarchal structure where cases are grouped based on their similarity forming Generalized Episodes (GE) and then differentiated or indexed below their respective GE based on the differences between instances. When a new case is added it is identified to its closest GE or

instance. If a matching instance is found the instances is reclassified into a new GE and the two cases are once again classified as instances below the new GE based on their differences. This forms a dynamic memory structure. Category-exemplar model is formed of categories with cases associated with them (Watson and Marir,1994).

To describe a cases relationship to a particular category, features are assigned different weights. This model utilizes three different types of links which point from features to cases or categories, from categories to their related cases and from categories to adjacent cases that differ by a few features. New cases are added by identifying the relevant categories and forming required links. If the differences are only diminutive the new case could be merged or neglected.

2.3.4 CBR Cycle

The essence of CBR lies in the application of a previous known solution to an existing problem which has been identified and defined, to generate a new solution. The steps performed in using Case Based Reasoning for solving a new problem can be described as a cyclical process shown in figure 3 (Aamodt and Plaza,1994). CBR cycle consists of four steps: retrieving a case similar to the problem case, reusing the retrieved case by modifying the solution because of differences between retrieved case and problem, revising the proposed solution by testing it in the real world or evaluating it with the help of an expert trainer or repairing it if it has failed, retaining the newly formed case and solution as a part of the database for future use. The steps are explained more below.

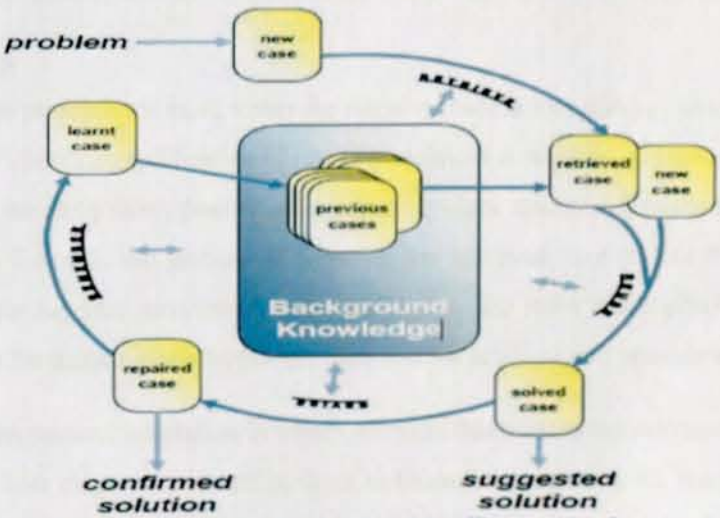


Figure 2 The CBR Cycle (adapted from Group for Artificial Intelligence Applications)

2.3.4.1 Retrieve Step

Retrieval step involves the retrieval of case/cases that are similar to the problem case from the database. It utilizes specific retrieval algorithms with the indices used to store the cases in the database to improve accuracy and speed. Heuristics like serial search and simulated parallel search are utilized to direct the search as partial matches are considered, while improving efficiency.

The development of retrieval stage involves the following (Watson and Marir,1994).

1. Identification of features interpreting the problem and collecting and inferring descriptors.

2. Search through direct matches and closest matches utilizing index structure of the case base.

3. Calculation of degree of similarity between possible cases to identify closest cases and perform initial matching.

4. Selection of the most similar case. Some standard retrieval techniques are Nearest Neighbor, Induction, Knowledge Guided Induction, and Template Retrieval. Retrieval process is usually divided into two phases, an initial partial matching search for possible solutions and a more detailed evaluation of partial matches for the most probable solution. A usual measure for an initial partial matching is the degree of importance of a particular feature on the case. Detailed evaluation is done based on the difference of key parameters of the retrieved cases to that of the problem. A ranking criterion is used to rank cases and thereby deduce the most similar case.

2.3.4.2 Reuse Step

After retrieval two possibilities exist, either the retrieved case is identified as an identical match to the problem case where no modification of retrieved solution is required and the retrieved case can be used as is, or, the more likely possibility, a relatively close case which needs to be modified to suit the problem Reuse is the process of adapting the retrieved case to suit the new problem. Adaptation can be: (a) structural/transformational, where the rules are applied to the retrieved solution to adjust for differences between the case and the problem and provide a new

solution, or (b) derivational adaptation in which the rules that created the solution for the retrieved case are used in their original or modified form to formulate a solution for the new problem. In derivational adaptation rules previously used to formulate the solution need to be stored with the

case. This method is best used for domains that are well understood and should be able to develop a solution from scratch.

2.3.4.3 Revise Step

This step is essential for CBR system to learn. In this phase the developed solution or predicted value is verified with real world results, which may take a long time, or a teacher (or expert) in some cases. During this learning phase either the predicted value is found to be accurate and the CBR cycle moves on to the retain stage, or the prediction is found to be inaccurate and the case is revised with the help of expert domain knowledge. Depending on how the prediction was made, the cause of the error and mistake in prediction may also be stored to prevent future occurrences and may be used to fortify the reuse process.

2.3.4.4 Retain Step

Retain presents the final step for the CBR cycle. During this step the solution to the problem is incorporated into the case base structure as a new case. A successful case forms a new entry while a failure can be formulated and stored as a new rule for the intermediate stages. When storing a case, it is essential to identify the information from the case that needs to be retained, and the form in which it is to be retained as well as how is it to be indexed so that the new case is integrated in the case base and can be easily identified for similar problems. If there is a small difference between the new case and the retrieved similar case the old case may be generalized to incorporate the new case. Sometimes an explanation of why a particular case was retrieved is also stored which aids in the modification or reuse step.

After the new case or rules are entered into the database the initial problem can be once again run to check if the correct solution is recalled as expected.

2.4 TOOLS FOR CBR

CBR Shell, myCBR, Jcolibri are some of the tools used in the implementation of CBR. This section gives an overview of the tools used.

2.4.1 CBR Shell

The AIAI CBR Shell is a generic tool for case-based reasoning. The tool performs classification based on case comparison. The parameters of the algorithm can be varied: the number of nearest

neighbors considered can be specified, the weights can be set manually, or the weights can be optimized by a genetic algorithm. The accuracy of the algorithm is measured by a leave-one-out evaluation.

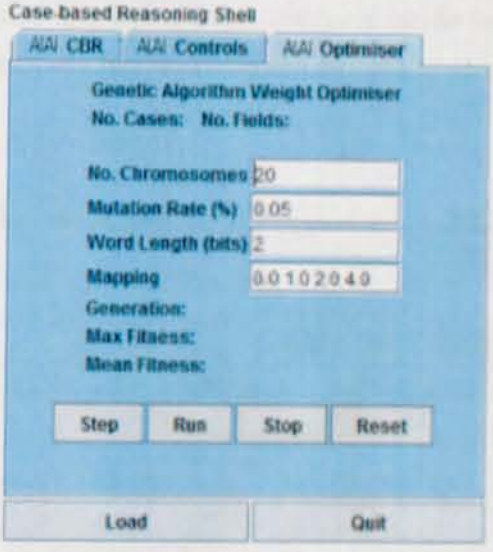


Figure 3 CBR Shell GUI Interface

2.4.2 jCOLIBRI

jCOLIBRI is just a white-box tool that licenses programmer users to have total control of the internal details of the software. jCOLIBRI symbolizes a case in a very general way. jCOLIBRI is a framework for developing various CBR applications. It is Java-based and uses JavaBeans technology for representation of case and automatic generation of user interfaces. jCOLIBRI supports full CBR cycle. A CBR application can be built by instantiating the framework, or through the GUI-based configuration tools, which allow one to form the application without writing a line of code. Nevertheless, if we want to build a very intricate CBR system or we need problem-solving methods that are not available in the framework, then, we could program new ways (methods) and include them into the framework, contributing them to other CBR system designers to use. At Retrieve stage, the N nearest cases are retrieved and there are five retrieval strategies, seven selection methods and over 30 kinds of text similarity functions and ontology. At

the Refusal stage, several adaptation methods are offered (direct proportion) and also in ontology. At Revise stage, methods for revision of cases as well new indexes (IDs) generation methods and methods for decision making (preference elicitation). At Retain stage, there are query retaining methods as a new case. jCOLIBRI allows retrieval form clustered and indexed case bases and program interfaces (connectors) are used to access text and XML format files, as well standard and data bases that are descriptive logics. These interfaces can be used for access of diagnostic systems databases. A graphically representation can be used to show CBR cases (Bel´en and Pedro, 2000).

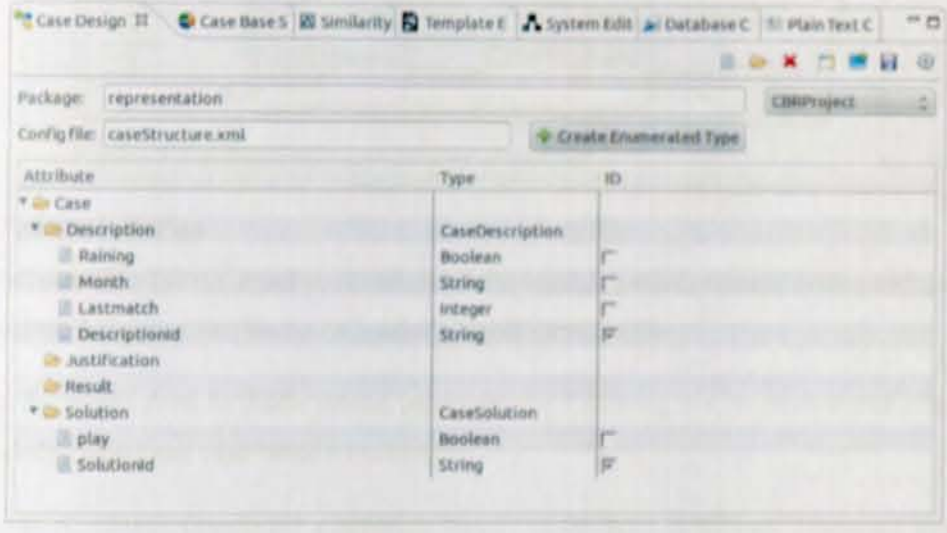


Figure 4 jCOLIBRI case designer tool

2.4.3 myCBR

MyCBR is an open-source similarity-based retrieval tool and software development kit (SDK). The framework my CBR supports description of cases with various attributes: numeric, character and string, logical, class type, etc. The cases templates are generated as classes or subclasses with a number of attributes, called slots. The CBR Cases are class objects described by its attributes. Each attribute can participate in the class with its value and weight that determine the significance of the attribute in relation to others. Attributes having zero weights are not considered when penetrating the case-base. In myCBR the case and their attributes can be generated either manually or automatically. The automatic generation of attributes (slots) is done through the import process of the Comma Separated Value (CSV) file.

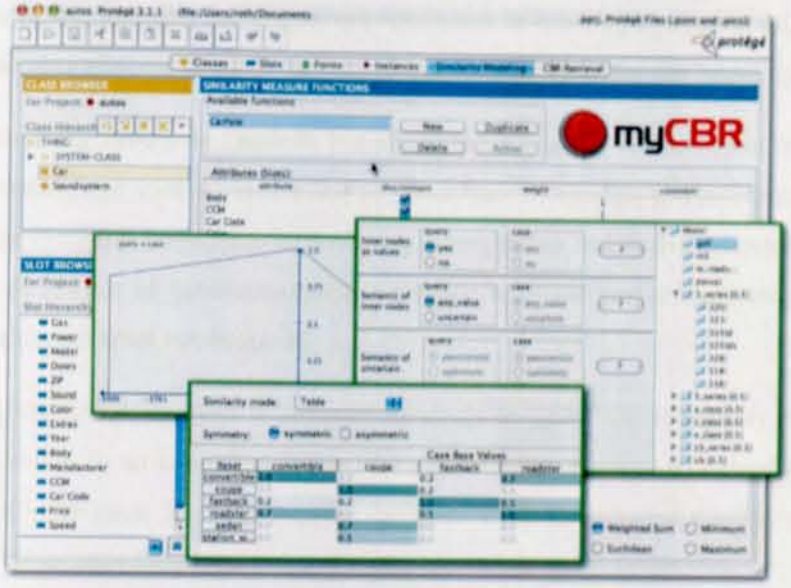


Figure 5 Similarity measure editors of myCBR

2.5 Related works

As the researcher has reviewed works related to the topic, knowledge-based system and case-based reasoning, there are some works on insider's threat identification.

From the works done in Addis Ababa university the following are research works related with knowledge based and case-based reasoning.

Meseret A, (2016) Conducted a research based on designed combined reasoning system for knowledge-based network intrusion detection. The combination of two reasoning systems, i.e. Case Based Reasoning (CBR) and Rule Based Reasoning (RBR) system was employed. To construct cases for a case-based reasoning a descriptive modeling and for generating rules for a rule-based reasoning predictive modeling were used. The KDD CUP 1999 Dataset has been used to train and test the combined reasoning system for knowledge-based-NID proposed in this research work.

Yemisrach H., (2010) conducted a research aiming of designing prototype, case-based reasoning in legal knowledge-based system that will advise in the investigation of children criminal cases. The prototype was developed using the Object-Oriented framework jCOLIBRI1.0. The CBR

model was unable to retrieve analogues previous cases in reaching a potential solution for decision making and also a means to adopt the current case of a problem for the future use.

Work in the early 1990's by Landreth has attempted to classify hackers as in "novices, students, tourists, crashers and thieves" in an effort to reveal their motivation and individual characteristics. The Hacker Profiling Project has equivalently attempted to codify the behavior / background of hackers with the use of questionnaires in a mission to reveal useful characteristics such as age, demographics, personal attributes, etc.

Kjaerland, M., (2006) analysis of reported incidents to CERT/CC to classify attacker operation related incidents. In an attempt to expand the classification window Kjaerland has presented the factors that were most likely to happen together. Work on attacker's behavior has also been conducted from a psychological point of view.

Shaw, E., 1999 has presented that elements of malicious cyber activity may be related with history of negative social and personal experiences, lack of social skills, sense of entitlement and ethical flexibility. Watters, P. ,2012 working from a similar perspective has attempted to apply a qualitative identification of cyber intruder profiles by conducting an ethnographic study of cyber-attacks.

Stelios K. The researcher conducted research mainly aiming to examine whether a case based rezoning approach can help security and forensic investigators to profile human attackers with regard to their behavioral, demographic and technical characteristics collected from real systems that are suspectable to intrusion attempts. On this work many features which are related with potential intruders, such as Skill level, risk aversion, education level, gender, predefined goal, speed mistakes, anti-forensic actions and success were evaluated in order to identify those attackers. The researcher selected case base reasoning technique with a pool of 87 real attack patterns to classify the background of the intruder.

Solomon M, 2015 conducted a study which proposes a context-aware insider threat prediction and prevention model based on the fraud Dimond, which can be used in real time combining approaches based on the inputs from computer science, psychology, and criminology. The proposed model uses context aware metadata language analyzer and user profiling assess the current context of insiders in order to identify users risk level for committing malicious act.

Many studies have been conducted in the literature regarding knowledge-based system and case-based reasoning. And from the above discussions, it can be concluded that most of the studies contributed in choosing tools for this study. Nevertheless, the studies focused on technical ways of the insider threat. That means they left the non-technical parts untouched to a larger extent which the major concern of this particular study.

On the other hand, the reviewed literatures specifically the studies that used behavioral models have emphasized more on the behavior of threats and not on the behavior of the insiders. But our study will focus on the behavior of the insiders themselves. Besides, the behavioral models reviewed in the literature have not been checked in practice and have not been implemented in a real situation.

Finally, the reviewed literatures used psychological indicators in identifying employees at risk using Bayesian network as their tool. However, the Bayesian network cannot learn and reason our , so cannot be used for future cases. And works do not provide technical mechanisms that can make use of an insider's characteristics in practice and possibly in real time. So, traditional technical security measures have always revolved around the characteristics of the attack rather than the attacker. In this regard, the current study will use knowledge acquisition tool by collecting important and selected information which are used to identify observable human behavior so that it can be contextualized and used to develop the knowledge base. This tool is chosen because it can use the knowledge and can guide in making future decisions.

Therefore, taking the above justifications in to account, this study will use CBR and knowledge-based system as its tool and study the insiders (attackers) behavior using knowledge acquisition which finally can be used as a guide for future decision making.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

The study follows design science research approach for the overall work of this study. The researchers, on the next sections has discussed What, How, and Why is each step of the research process done in detail. The fundamental principle of design science research is that knowledge and

understanding of a design problem and its solution are acquired in the building and application of an artifact. (Alan Hevner, 2010).

We use the Information Systems Design Research (ISDR) approach as proposed in Peffers et al. (2008) as a foundation. An overview of the design research process model is shown in figure 1 Problem identification and motivation, objective of the solution, design and development, demonstration, evaluation and finally communications of the design science research process steps are used.

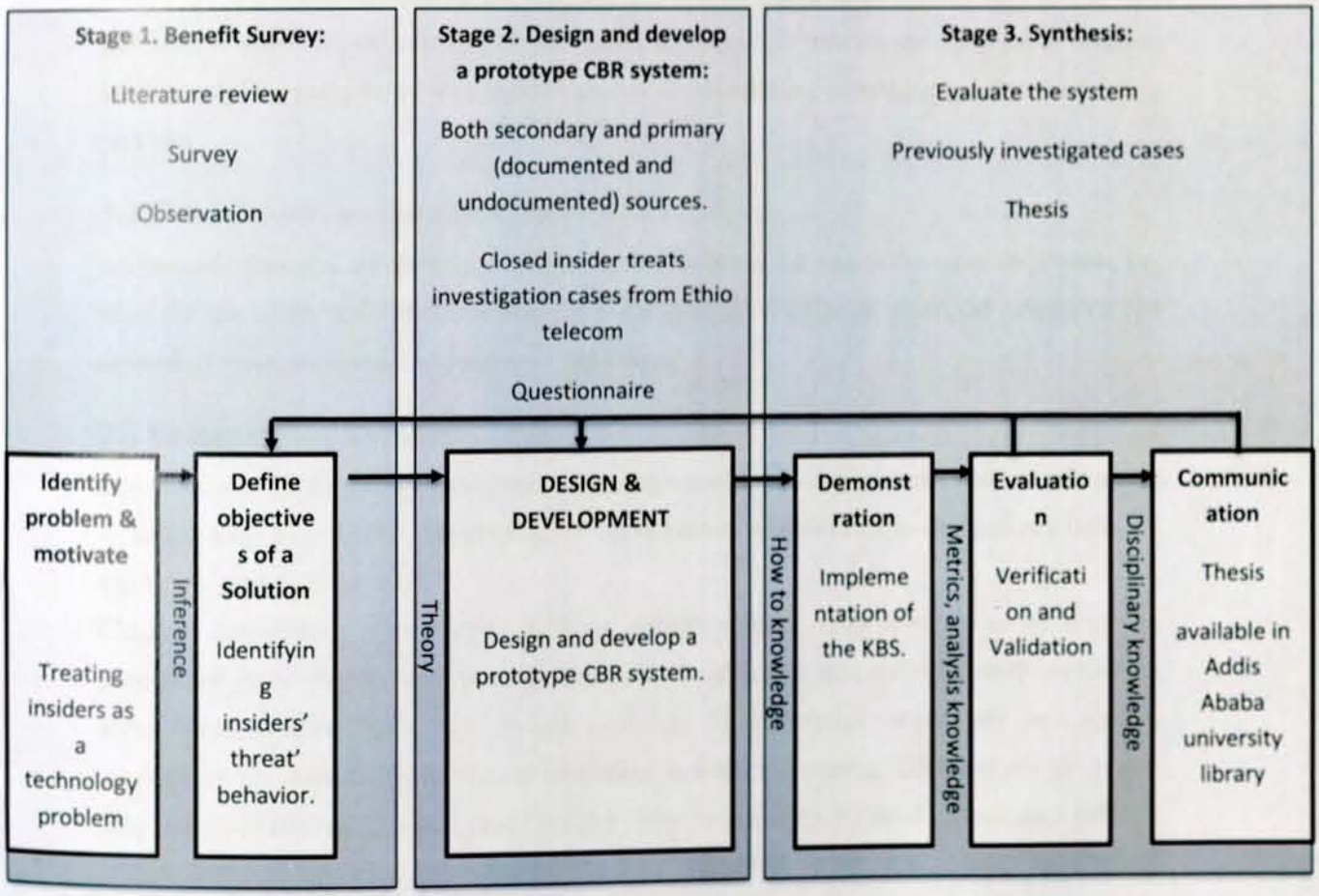


Figure 6Initial design science method process model (Based on Peffers et al. 2008)

In stage one we begin with a systematic literature review followed by a survey. In stage two we conduct both secondary and primary (documented and undocumented) data analysis and design and develop a prototype CBR system artefact. In stage three we have evaluated the prototype CBR system and enhance it through further design and development.

3.1 Identify problem and motivate

Wide literature reviews from different sources like articles, books, researches and the Internet are conducted in order to identify the problem on the area, and also to have detailed knowledge on techniques and tools of knowledge-based system with respect to case based reasoning approach. As discussed in detail above on section 1.2 and 1.3 the reviews conducted indicates that insider threats are not a technological problem and many related works treat insiders as a technology problem, in which this attitude ignores the human aspects of motivation and behavior of insiders, for this result the researchers were highly motived on contributing something to solve the existing problem.

3.2 Define objectives of a Solution

As research objective are the results sought the researcher at the end of the research process, i.e. what the researcher will be able to achieve at the end of the research study, the researcher has defined general and specific objectives of the study.

3.3 Design & Development

The researcher preferred case-based reasoning rather than rule-based system is that, we are trying to study a case related with human behavior. So as human behavior can be changed any time, we can't give a specific rule to it.

Classical knowledge- or rule-based decision support systems draw conclusions by applying generalized rules, step-by-step, starting from scratch. Although successful in many application areas, such systems have met several problems in knowledge acquisition and system implementation. Inspired by the role of reminding in human reasoning, CBR systems have been proposed as an alternative to rule-based systems, where knowledge or rule elicitation are a difficult or intractable process. In principle, the CBR approach takes a different view, in that reasoning and problem-solving are performed by applying the experience that a system has acquired. This approach focuses on how to exploit human experience, instead of rules, in problem- solving, and

thus improving the performance of decision support systems. In brief, reasoning in CBR is based on experience or remembering.

In CBR, a primary knowledge, stored in memory, is not compiled from rules, but a set of structured Cases. These cases represent an experience or lesson that, under which situations and to what problems, some specific solutions have been derived in the past to achieve the goals of the reasoner, and the effects after the solutions have been applied. When a new problem is presented to the system, a new solution is proposed by retrieving the most relevant old cases and adapting them to fit new situations, which is then introduced as a new case into the system in order to enrich the case base. Therefore, a case-based reasoner solves new problems by adapting solutions that were used to solve old problems and with efficient adaptation strategies and a proper complement of new cases, a CBR reasoner is expected to work more and more effectively.

3.3.1 Sampling Techniques

Purposive sampling is one of the most common sampling techniques in qualitative research in which participants group are decided to pre-selected criteria relevant to a particular research question. Purposive sampling helps the researcher to use different characteristics to select the subject of the study. (Mack et al, 2005, P.6). So, in order to acquire knowledge required for the development of the system, the researcher subjectively selected experts with knowledge of the domain.

3.3.2 Methods of Data Collection

The various methods of knowledge acquisition from different sources, knowledge representation and system development that are used in this study are discussed below.

In this study to acquire the needed knowledge, both secondary and primary (documented and undocumented) sources of knowledge are used. Primary knowledge is gathered from documented closed insider treat investigation cases from Ethio telecom. In addition, knowledge is gathered from two groups of domain experts, the first group are experts like attorney, sociologist and psychologist, which are participated on identifying additional human observable behaviors that can be used in identifying at risk employees. On the other hand, knowledge has been acquired from Coaches, Supervisors, Managers, Officers, and Coworkers of those insiders who was found guilty and suspended from Ethio telecom. In the same way, secondary sources of knowledge are collected by using document analysis. Interview (both structured and unstructured) is used to

collect tacit knowledge from the domain experts. In addition, critiquing (analyzing) elicitation methods is used to purify the collected knowledge. Moreover, secondary sources of knowledge are gathered from the Internet, research papers and articles by using document analysis technique.

3.4 Demonstration

Demonstrate the use of the artifact to solve one or more instances of the problem. This could involve its use in experimentation, simulation, case study, proof, or other appropriate activity. Here as the researcher has acquired all cases with their necessary information needed, the next step is to codify and represent those knowledge's using a suitable representational model for the intended case-based reasoning system. So here using jCOLIBRI; case structures, data types, connectors, and tasks are managed in order to make the application functional, so that we can check wither the system performs the expected task.

3.5 Evaluation

System evaluation is a process of determining the quality of the knowledge base system and the advice it provides. A knowledge base system evaluation involves two processes: Verification and Validation. Verification is the process of inspecting the system looking for any error and to see how well the system works as per the requirements specification. During validation the system is evaluated whether it is useful or not. For this purpose, test cases are prepared and given to the system and to the experts who initially provided the knowledge. The answer from the system and the experts are compared to see how accurate the system is (Amir S., 2004). For the evaluation of the user acceptance testing, different researchers used different evaluation criteria. On our work we have customized and adapted evaluation criteria suggested by Dawit (2015), Alemu (2010), and Seblewongel based on the ISO standard 9126.

3.6 Communication

As this final stage is the process of delivering what is understood and the overall result from the work, the work presented to Ethio telecom information and network security division the researcher has published the work in a hard and soft copy which will be available on Addis Ababa university library.

CHAPTER FOUR

KNOWLEDGE ACQUISITION AND MODELLING

4.1 Knowledge acquisition

Knowledge acquisition is the process of collecting important and selected information, which is used to develop the knowledge base. The case-based reasoning, which is going to be developed on insider threat that would be used by security professionals in evaluating problems, utilizing the experience in the particular field. During the knowledge acquisition process, the knowledge that a KBS needs in order to perform a task, is defined in such a way that a computer program can represent and adequately use that knowledge. Knowledge acquisition involves, in our view, at least the following activities: eliciting the knowledge in an informal-usually verbal-form, interpreting the elicited data using some conceptual framework, and formalizing the conceptualizations in such way that the program can use the knowledge.

The knowledge acquisition process is usually comprised of three principal stages:

1. Knowledge elicitation is the interaction between the expert and the knowledge engineer/program to elicit the expert knowledge in some systematic way.

2. The knowledge thus obtained is usually stored in some form of human friendly intermediate representation.

3. The intermediate representation of the knowledge is then compiled into an executable form that the inference engine can process.

4.1.1 Knowledge Acquisition from relevant Document

The documents that the researcher refers include:

- Articles that are available in different sites
- Researches that are done using case-based reasoning.
- Ethio telecom internal communication and legal documents.

Additionally, the researcher has tried to identify variables that are considered as an insider threats which are identical in different types of cases. Most of the variables identified by other researchers considers only the behavioral aspect of the person/employee.

4.1.2 Knowledge Acquisition from Insider Threat Cases

Knowledge acquisition from domain experts and other relevant documents is found to be very important and vital and incorporated in this study. Meanwhile, the main knowledge that is used for the case-based reasoning systems were collected from insider fraud activities (cases) which happened in the product and services of Ethio telecom. Consequently, the variables that are identified from those cases are used as the main variables for the insider threat identification in this study. In addition, variables that are identified through semi structured interview with the domain experts and other related documents before are also used.

The researcher has referred different reports from different departments of ethio telecom which are related with fraudulent employees. As the researcher's investigation, seven cases were identified as per the type of fraud committed. here below is their list with their explanation.

1. Benefit Related Fraud

Those fraud types are committed by employees which has full privilege to do the action legally. In this type of fraud, the department information systems of the company take the major percent of the fraud. Mainly those frauds are done by releasing different service benefits illegally on different products. Releasing or attaching benefits like free internet, free SMS and free voice.

2. False Certification Fraud

This type of fraud, as the researcher's work, it has been seen on many departments of ethio telecom other than the rest fraud types. The cases on the researcher hand shows that employees with different false certification were identified and necessary measurement was taken by the concerned body. Different medical, receipts, educational and decision letters were among the false certification fraud done by the employees.

3. Inventory Related Fraud

Employees which steals products from the company either by physically taking it or diverting it in some other way were the participant of this type of fraud. Inventory thefts like cash money, different telecom equipment were the common ones.

4. SIM Box Related Fraud

SIM box related frauds are done mostly by employees who has chain with those persons committing SIM box fraud all over the country. Investigated cases shows that the employees working on the company's sales department takes the first rank by engaging themselves on such actions. The fraud is done by selling thousands of SIM cards which has false profile, which includes owners' photo, full name, address, identification card number, and the likes.

5. SIM Card Related Fraud

Preforming SIM card replacement, ownership change, suspension, and release without the confirmation (approval) of the customer are the main fraud done under SIM card related fraud.

6. VAS related fraud

The company's value-added services (VAS) like short code service, Vanity numbers, CRBT, are among the main target of the insiders under this type of frauds. On such frauds insiders intentionally force the system to stop working properly as designed. For example, in short code services, after customers subscribe for one service, and latter while trying to unsubscribe it will not work.

7. Data theft related fraud

Data theft is also the other type of employee fraud observed on Ethio. Different types of customers and the companies' sensitive data are being stolen and transferred to third party illegally. This type of fraud mainly take place on Customer service department.

4.1.3 knowledge Acquisition from Domain Experts

As the researcher is looking for cases that happened in the past with the detail of each cases and the system case-based reasoning by itself is dependent on different types of knowledge that are stored as past solved problems. So, the expert's knowledge is a vital thing.

On this work we have two groups of domain experts, the first group are experts like attorney, sociologist and psychologist, which are participated on identifying additional human observable behaviors that can be used in identifying at risk employees. On the other hand, after the researcher has finished case acquisition and attribute selection, knowledge has to be acquired from Coaches, Supervisors, Managers, Officers, and Coworkers of those insiders who was found guilty and

suspended from Ethio telecom. So, knowledge was acquired from both group of experts, and the results are discussed below in detail.

4.1.3.1 Knowledge Acquisition from Domain Experts group 1

The researcher has contacted domain experts who are expected to have knowledge related with human behavior. On this part we have a detail discussion with three psychologists, two attorneys, one sociologist from Addis Ababa University, FDRE attorney general and self-employed personnel's, in order to get relevant information needed. The researcher has a successful discussion with the listed domain experts. First those experts have got a brief explanation on the work and were asked to put their assumption on the behavioral indicators that the researcher brought from relevant documents with respect to our country. Next, they were asked to write down any other behavioral indicators that, insiders show while he/she is in a fraudulent activity. The main points we got from the domain experts are discussed below.

Discussion with a Lawyer

As per the discussion the researcher made with the Lawyer, the researcher has got important points. The professional mainly focus on criminology while discussing the issue. He told the researcher that international studies show that most crimes are committed by depending on some situation. Most organizational criminal cases investigation shows that the process focusses on factors such as: -

- ✓ The time frame/season when the crime committed.
- ✓ The type of the service or product, the crime pointed.
- ✓ Product/service release time.
- ✓ The experience and skill level of the insider/employee.
- ✓ Motive of the insider to commit the crime.
- ✓ The department where the crime committed

The researcher also asked if they have any additional human observable behavior which can help to identify at risk employees of one's company. Unexpected acquisition of wealth, generosity, over

care act for the organization, interest to trainee employees and also higher officials can help the process of the identification.

Discussion with a Psychologist

The researcher has also obtained some information from a discussion with a psychologist, regarding to some possible additional human observable behaviors that can be seen on employees committing fraudulent activities. Accordingly, a person intended to commit fraudulent activities has the potential to show the following additional human observable behaviors as has been identified by the psychologist:

- ✓ Inattentiveness/hyperactivity
- ✓ Deception
- ✓ Malingering

Discussion with the Sociologist

The same questions asked for other professionals were also asked for the sociologist. The researcher has tried to put the summery of the discussion as below.

Sociology mainly studies the factor and motive at the back of any crimes and fraudulent activities, rather than the psychologically observable behaviors. Mainly sociologists believe that humans start learning and having their personalities firstly from their families. There are pull and push factors for such crimes/frauds to be committed. From those factors

- ✓ Economic factors
- ✓ Social values
- ✓ Peer pressure
- ✓ The need for acceptance
- ✓ Accepting all role model personalities right.
- ✓ Multiple personalities disorder

So generally, as per the discussion, the researchers believe that the sociological aspect is very important while studying the root cause of each crimes.

4.1.3.2 knowledge Acquisition from Domain Experts group 2

Domain experts under this group are immediate boss of those insiders who was found guilty and suspended from Ethio telecom in earlier times. As the researcher is building a case base based on how frequent the selected human observable behaviors were observed on those fraudulent employees, we have prepared a 6-point Likert scale questioner survey. The survey was distributed for selected 44 persons including ten coaches, twenty coworkers, nine Managers, and five officers of those insiders who was found guilty and suspended from their job. SPSS tool was used in order to make the descriptive analysis of the collected data.

4.2 Knowledge Modeling

After the knowledge is acquired from insider cases, two group of domain experts, and other relevant documents, the next step is modeling the knowledge. Knowledge modeling mainly involves the steps of organizing and structuring the acquired knowledge while the knowledge acquisition process. The researcher used deductive approach while identifying knowledge items gathered from different sources, and to model those acquired knowledge, hierarchical tree structure was used.

4.2.1 Case Concept for Depicting employee's behavior towards potential frauds to be committed

In the process of depicting employee's behavior towards potential frauds to be committed, human observable behaviors that employees show at working place, observation frequency of those indicators, employee's department will be checked. Many observed frauds that was committed were done department wise. The main reason for this was that, privileges of different systems was given to employees according to Ethio telecoms organizational structure, for this reason

investigated fraud cases in one department were unique from cases committed on other departments. The general Concept for depicting employee's behavior is shown below on figure 7.

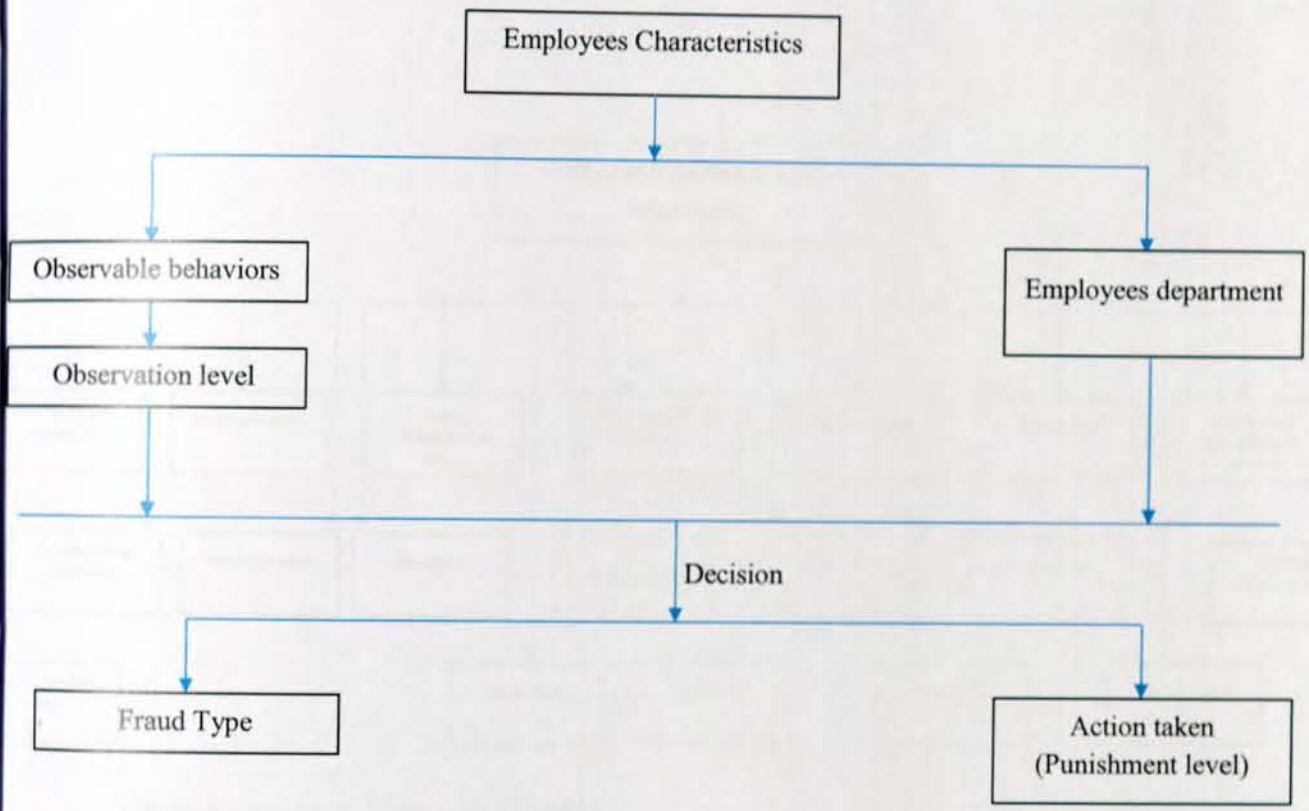


Figure 7 General Concept for identifying insiders threat behavior

The twenty-human observable behaviors indicator, observation frequency of those indicators, employees working department, and possible punishments to be taken are discussed below.

4.2.1.1 Employees Observable behaviors

As shown below on figure 8 there are twenty indicators of those observable behaviors and one identification attribute, that is the current working department of the employee. So, each of the 20-human observable behaviors was rated based on how frequent they were seen on earlier investigated and suspended insiders in Ethio telecom. On our case base 70 observations of those insiders under seven different fraud types were stored, and served as a reference when a new query come to the system. Based on the above stated twenty-one attribute values, the CBR system will

come to decision on retrieving the most similar cases with the type of fraud they committed and the punishment they receive.

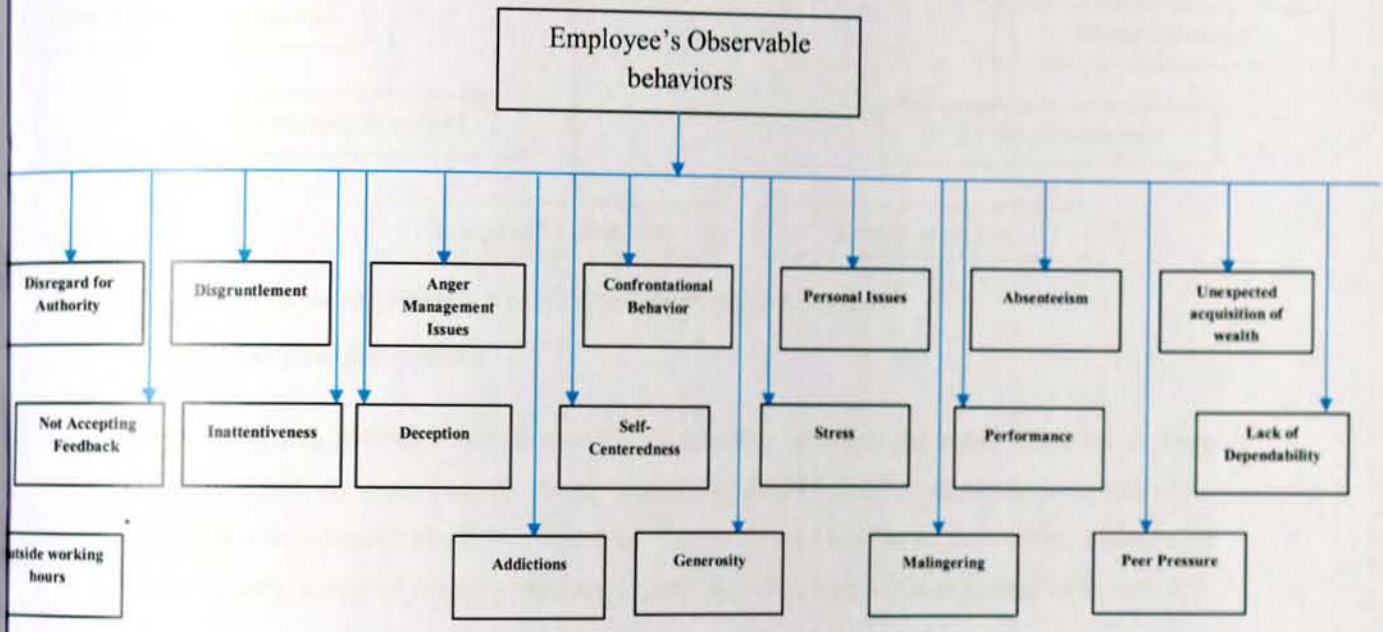


Figure 8 Employees Observable behaviors

4.2.1.2 Observation level

Observation frequency of each employee Observable behaviors are rated by using a six-point Likert scale questionnaire. As shown below on figure 9 the frequency of the employee showing one behavior will be used as an input value for each twenty attributes of observable behaviors.

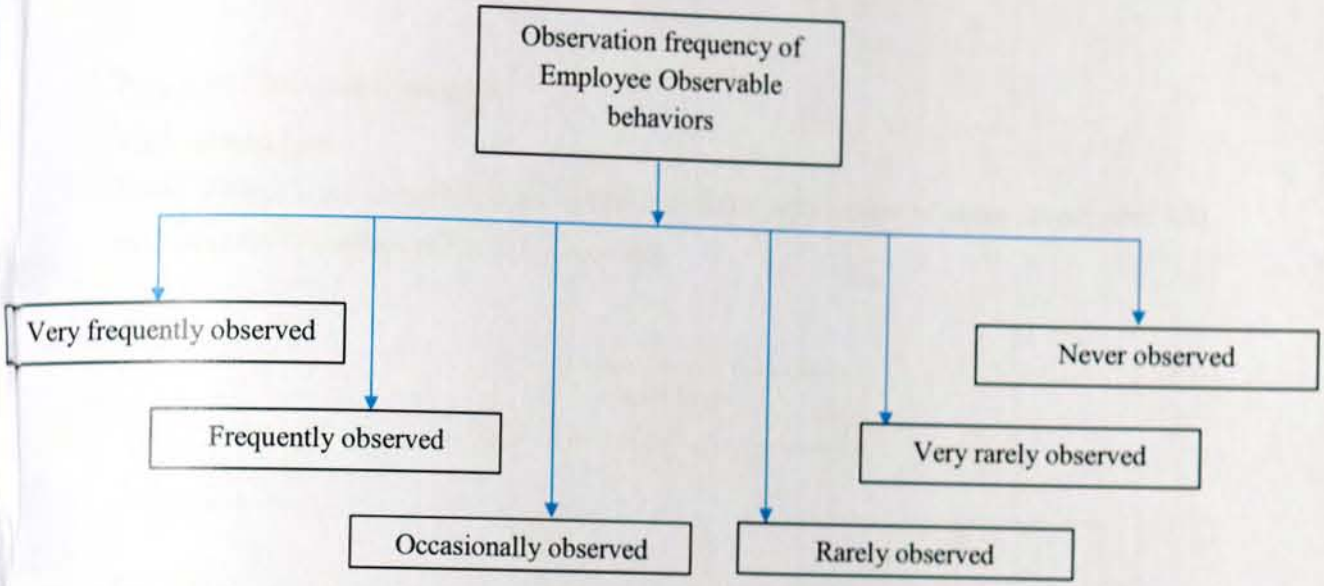


Figure 9 Observation frequency of Employee Observable behaviors

4.2.1.3 Employees department

While depicting fraudulent employees the department of employee being observed is very important input. Analysis from the stored cases shows that the fraud types are more dependent on employee's department. As shown below on figure 10, we used the organizational structure of Ethio telecom, we found from the company higher official directly while modeling the knowledge.

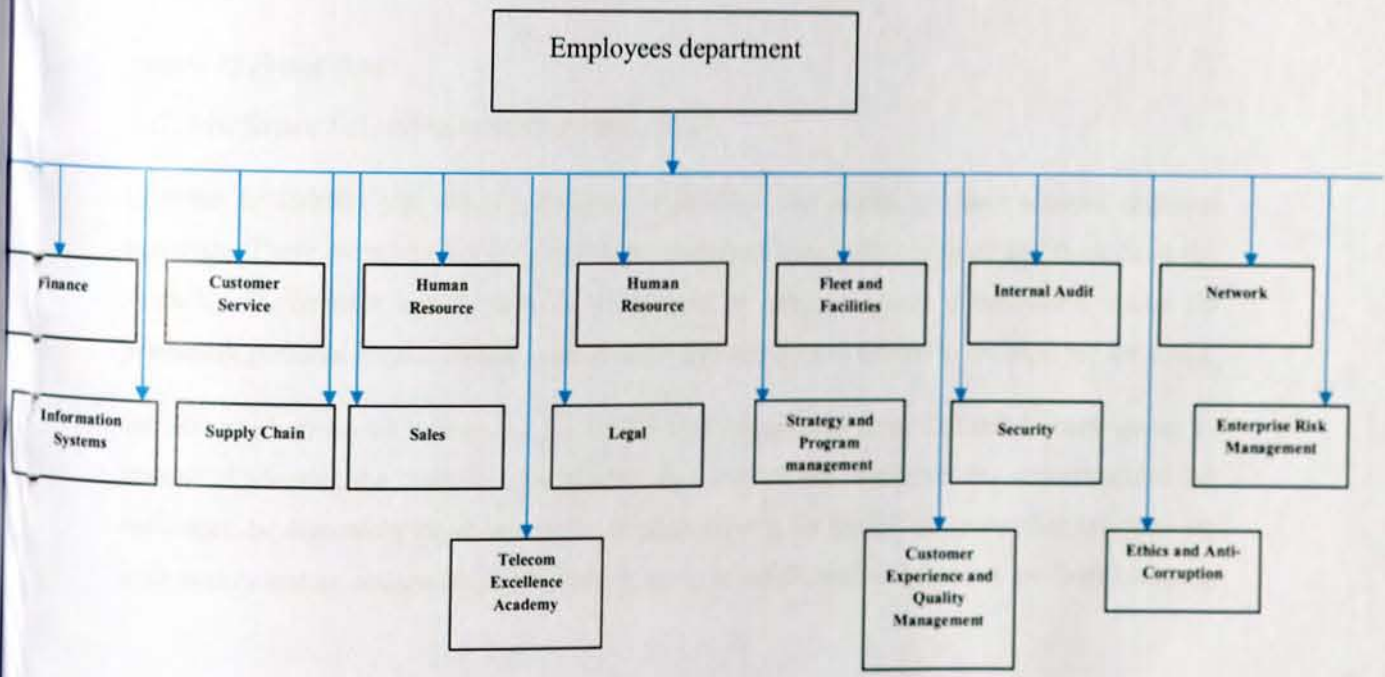


Figure 10 Employees department

4.2.1.4 Fraud type

These attributes are classified under solution attribute, with values of seven investigated and proved frauds committed earlier to the company.

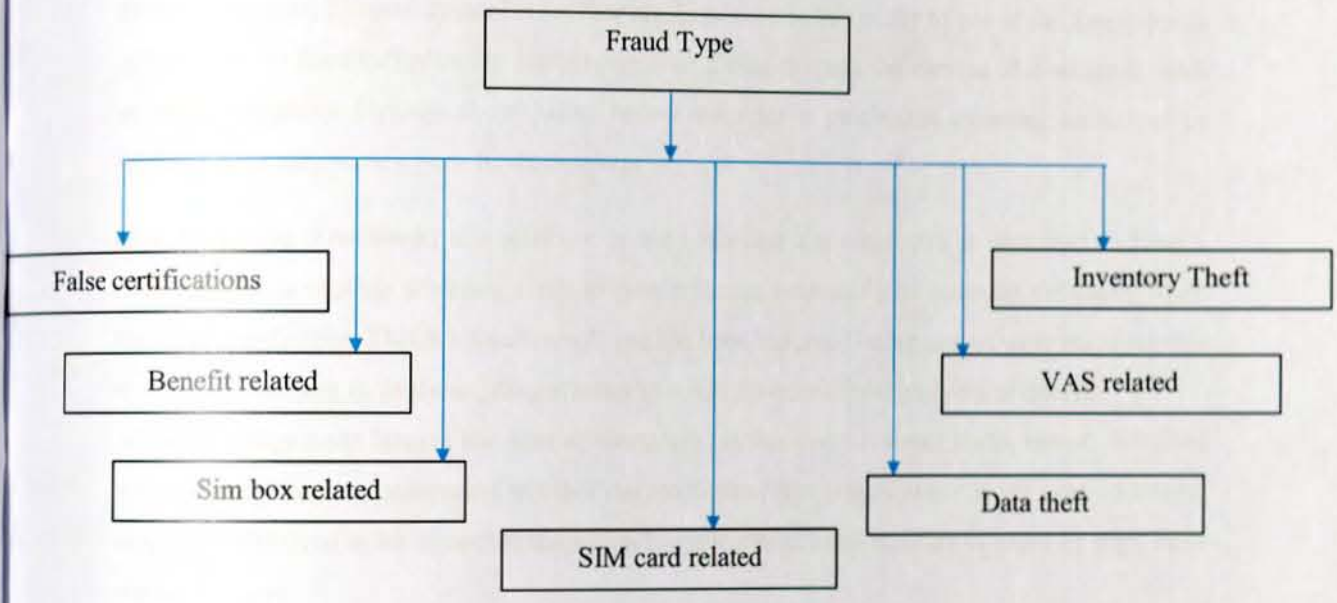


Figure 11 Fraud Type

4.3. Attribute Selection and Case Structure

In order to identify and select indicators of humans, the researcher have referred different materials. There are some researchers that worked on human behavior profiling, from those the work by FL Greitzer and LJ kangas (identifying at risk employees a behavioral model for predicting potential insider threats) were found very relevant and related to the topic we are doing.

As discussed above on section 3.1.3.1 knowledge Acquisition from Domain Experts group 1, instead of adopting the indicators we found from literature, the researcher has contextualized the indicators, be discussing together with the domain experts. So finally, the researcher has come up with twenty human observable behavior indicators, in which twelve indicators are from literature

and eight indicators are from the domain experts so they are used in order to identify the at-risk employees. The purpose and description of each attribute are discussed here under.

Disregard for Authority: this attribute will help to gather information whether the employee disregards rules, authority or policies and also whether the employee feels above the rules or that they only apply to others.

Disgruntlement: Disgruntlement is another attribute used in this study to see if the Employee is observed to be dissatisfied in the current position; shows chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid or undervalued; may have a poor fit with current job.

Not Accepting Feedback: this attribute is used whether the employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message is delivered. This is because employee has been observed being unwilling to acknowledge errors; or admitting to mistakes; may attempt to cover up errors through lying or deceit.

Anger Management Issues: the other attribute used in this study is anger management. We used anger management to understand whether the employee often allows anger to get pent up inside; employee observed to have trouble managing lingering emotional feelings of anger or rage; hold strong grudges.

Disengagement: to understand whether the employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoids meetings, this attribute (disengagement) is used.

Performance: performance is also one of the important attribute that this study use to understand whether the employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance. Because low performance may lead to such acts.

Stress: it is expected that if the employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling, so to have information on these behaviors we have used the attribute.

Confrontational Behavior: To assess whether the employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation, this attribute is used as a tool.

Personal Issues: To know the level of an employee difficulty on keeping personal issues separate from work, and the interfere of these issues with work we have used this attribute.

Self-Centeredness: To know the employee attitude towards disregard needs or wishes of others, concerned primarily with own interests and welfare the attribute (Self-Centeredness) is used.

Lack of Dependability: To observe whether the employee is unable to keep commitments /promises; unworthy of trust this attribute is used as a tool.

Absenteeism: This attribute is used in order to help us on understanding whether the employee has exhibited chronic unexplained absenteeism.

So generally, as per the discussion, the researchers believe that the sociological aspect will be very important while studying the root cause of each crimes.

Unexpected acquisition of wealth: Employee has exhibited with unusual wealth with their income. Such as buying new car, wearing brand materials, buying house and the like.

Inattentiveness Employee exhibits impulsive, amoral, uncontrolled and detached from normal relationships.

Deception: Employee told lies, said nasty things, blackmailed someone or told about other peoples that were not true.

Malingering: Employee deliberately falsifying the symptoms of illness for secondary gain, exaggeration of existing depressive symptoms or failure to make enough effort in a cognitive task.

Addictions: Employee exhibited being addicted on different on different types of addictions. Like drug, alcohol, chat and the likes.

Peer Pressure: The employee has a feeling that one must do the same things as other people of one's age and social group in order to be liked or respected by them.

Generosity: The employee exhibited showing a readiness to give more of something, especially money, than is strictly necessary or expected.

Outside working hours: The employee is exhibited coming to office outside the company's working hours.

As shown below on table 1 the researcher finally come up with description, one identification, and two solution attributes.

Table 1 Features and dimensions Surface representing a case

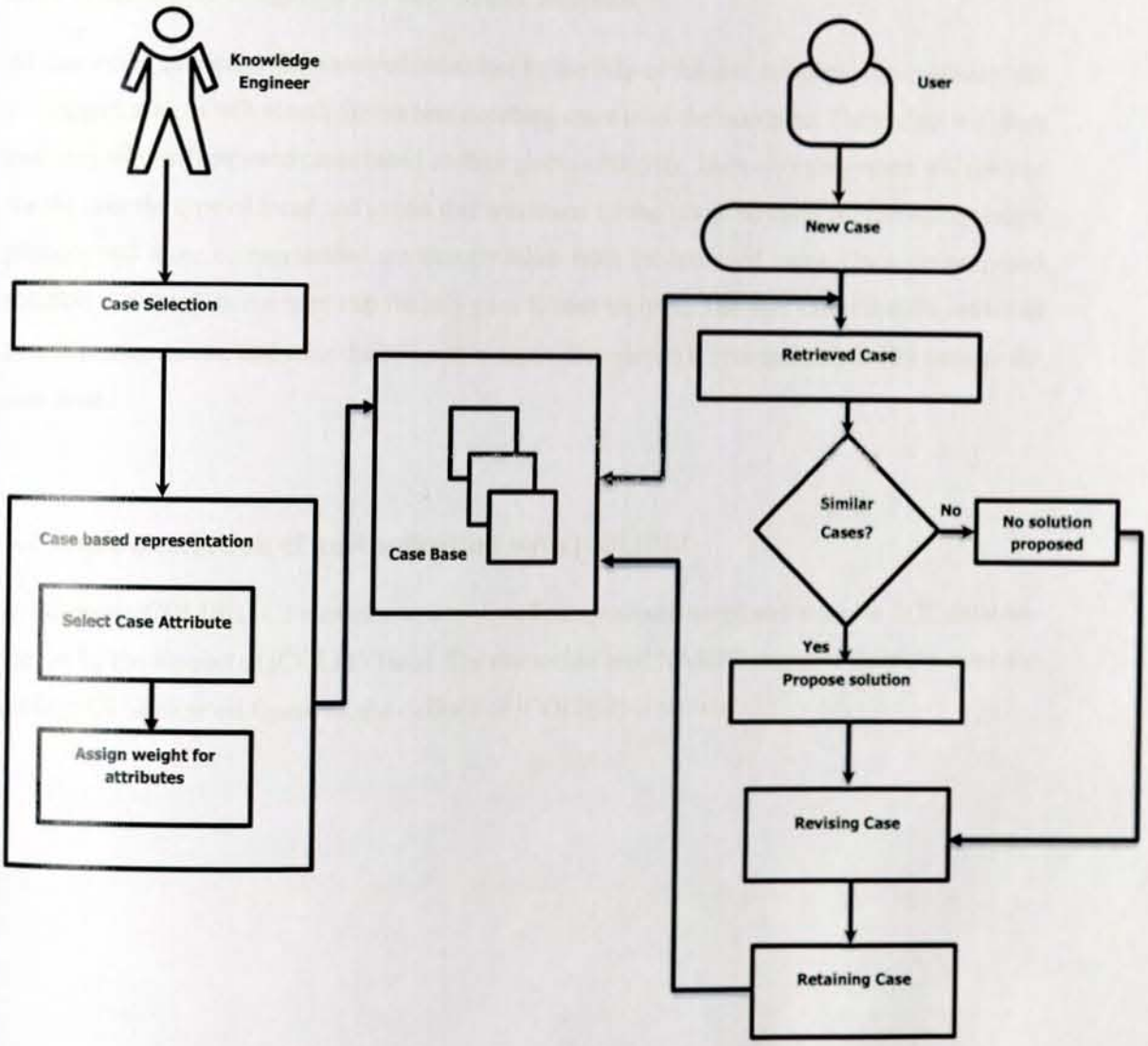
Case Attributes	Parameter of case
Disregard for Authority	Description
Disgruntlement	Description
Anger Management Issues	Description
Confrontational Behavior	Description
Disengagement	Description
Not Accepting Criticism	Description
Self-Centeredness	Description
Stress	Description
Performance	Description
Lack of Dependability	Description
Personal Issues	Description
Absenteeism	Description
Unexpected acquisition of wealth	Description
Inattentiveness	Description
Deception	Description
Malingering	Description
Addictions	Description
Peer Pressure	Description
Generosity	Description
Outside working hours	Description
Department	Identification
Fraud Type	Solution
Taken Action	Solution

CHAPTER FIVE

IMPLEMENTAION, TESTING AND EVALUATION

5.1. Designing of the Prototype

As the researcher has acquired all cases with their necessary information needed, the next step is to codify and represent those knowledge's using a suitable representational model for the intended case-based reasoning system. But before proceeding to the next action, that is the implementation phase, designing the architecture of the CBR system will come first. So below the researcher has presented the architecture with its explanation.



On the knowledge engineering side, the researcher has first made selection of cases, and then figured out attributes that can indicate human observable behaviors, which are identified internationally by the domain experts. Though there are listed human observable behaviors which are seen on fraudulent employees, it doesn't mean that those behaviors will represent our country. So, instead of adopting those identified and listed indicators, the researcher has tried to contextualize them by discussing with our country domain experts. Those experts were first asked to evaluate with those internationally identified behavioral indicators can represent our context or not. Then those domain experts were asked for any additional behavioral indicators that can be used on identifying at risk employee of an organization. After case attribute selection have been done, weights were assigned to the selected case attributes.

At first as the user enter the observed behaviors by the help of the user interface, automatically the configured system will search for the best matching cases from the case base. The system will then rank any relevant retrieved cases based on their global similarity. Then after the system will display for the user the type of fraud and action that was taken for the retrieved cases for recommendation purpose and those recommended are directly taken from the retrieved cases. Once the proposed solution is displayed. the next step directly goes to case revision. The user can revise the retrieved case for amendment, and after the revision is made, knowledge is retained and finally store to the case base.

5.2 Implementation of an Application with jCOLIBRI

In this work jCOLIBRI 1.1 was used as a tool, and cases are structured and stored in SQL database format by the support of jCOLIBRI tool. The researcher used XAMPP server to build the database on MySQL. Below on figure 13, the outlook of jCOLIBRI is shown.

Figure 12 Main window of jCOLIBRI

To make the system easy for use the researcher used user component extension from the tool, so that the users can easily insert their query easily from the lists available in a dropdown menu.

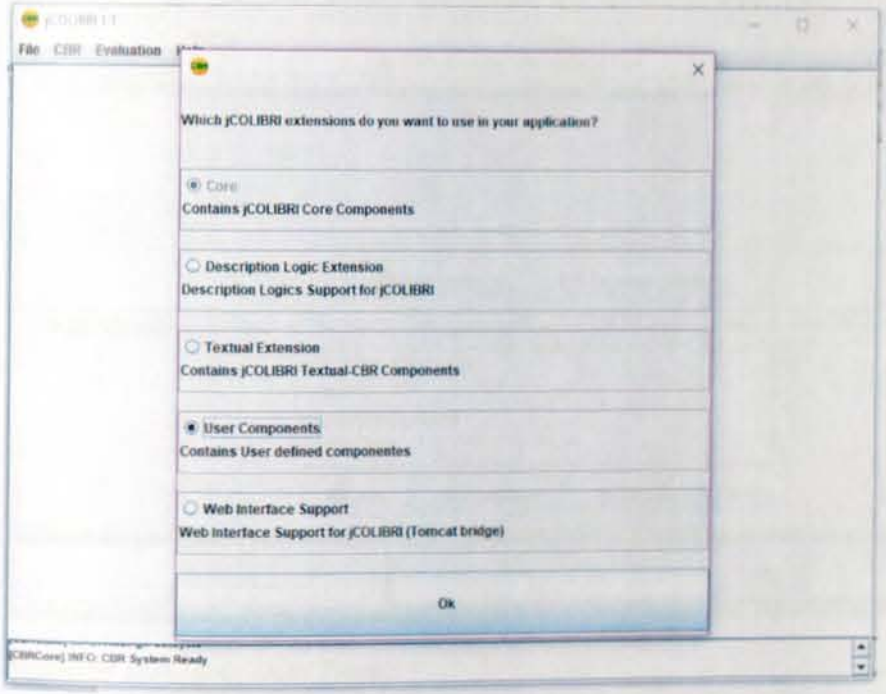


Figure 13 Selecting user component as an extension on jCOLIBRI

5.2.1 Managing Data Types

As shown above on figure 15 the researcher selected user component extension, so the data type has to be managed in order to configure the system with user-defined set of values. Two Enumerated data type variables has been added and managed to the system. The first variable named ObservationEnum have set of values Very frequently observed, frequently observed, occasionally observed, rarely observed, very rarely observed and Never observed. The second variable named DepartmentsEnum has set of values such as Finance, Human Resource, Marketing, International Business, Network, Information Systems, Supply Chain Sales, Customer Service, Fleet and Facilities, Internal Audit, Legal, Security, Enterprise Risk Management, Customer Experience and Quality Management, Strategy and Program management, Telecom Excellence Academy, and Ethics and Anti-Corruption.

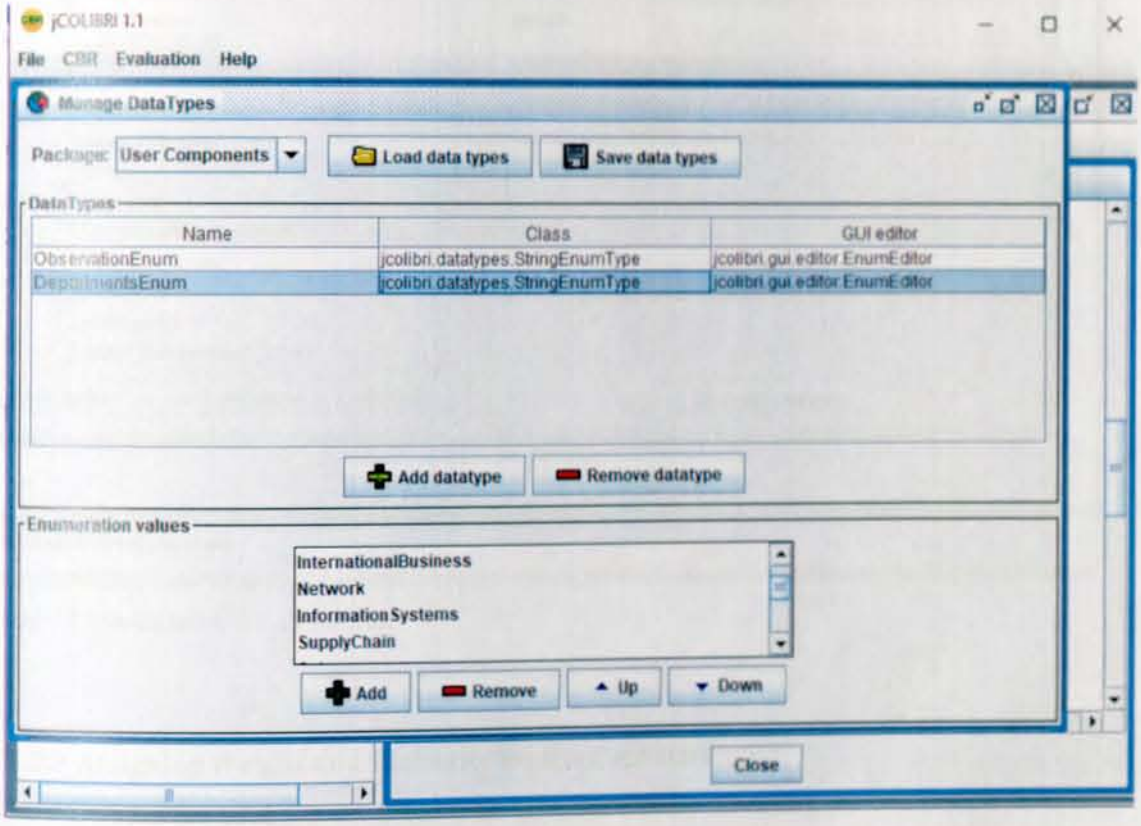


Figure 14 Managing Data Types

5.2.2 Managing Case structures

As defining case structure is one of the features of jCOLIBRI, the researcher has defined the selected attributes by inserting their correct definitions on the window ready for managing case structures as shown below on figure 16 On this step name, type, weight, local similarity, and global similarity of the selected attributes are managed correctly.

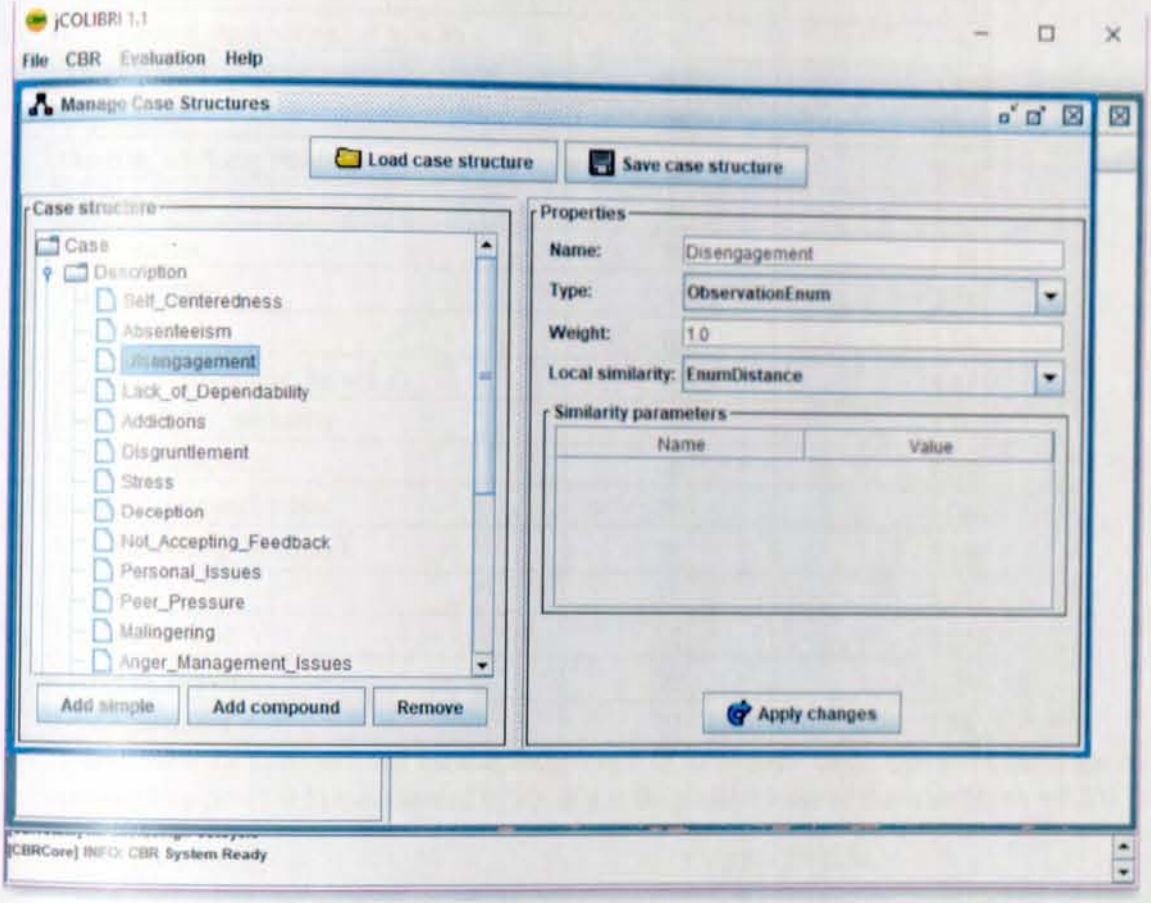


Figure 15 Managing Case structures

5.2.3 Assigning Weight and Similarity for the Case attributes

As the researcher used 6-point Likert scale type scale while surveying the observation level of each selected attributes, it is must to use the standard way while assigning weight for those case attributes. So by using the descriptive analysis output from SPSS, the standard ranges for weight assignment was derived. Table 2 below shows us the average mean of each attributes.

Table 2 Descriptive Statistics from SPSS

Descriptive Statistics		
Case Attributes	N	Mean
Addictions	70	4.23
Confrontational_Behavior	70	3.89
Inattentiveness	70	3.73
Unexpected_acquisition_of_wealth	70	3.70
Absenteeism	70	3.51
Generosity	70	3.44
Outside_working_hours	70	3.40
Performance	70	3.33
Malingering	70	3.24
Peer_Pressure	70	3.23
Deception	70	3.14
Anger_Management_Issues	70	3.11
Disregard_for_authority	70	3.10
Self_Centeredness	70	3.07
Lack_of_Dependability	70	3.04
Not_Accepting_Feedback	70	2.99
Stress	70	2.91
Disengagement	70	2.84
Personal_Issues	70	2.79
Disgruntlement	70	2.26

To determine the minimum and the maximum length of the 6-point Likert type scale, the range is calculated by (6 − 1 = 5) then divided by six as it is the greatest value of the scale (4 ÷ 6 = 0.83)

- 6 – 5 = 0.83
- 4.9 – 4 = 0.66
- 3.9 – 3 = 0.5
- 2.9 – 2 = 0.3
- 1.9 – 1 = 0.16
- 0.9 – 0 = 0

By using the above standard range, the researcher has assigned weights for each attributes accordingly. Case attributes such as Confrontational, Behavior, Inattentiveness Unexpected acquisition of wealth, Absenteeism, Generosity, outside working hours, Performance, Malingering, Peer Pressure, Deception, Anger Management Issues, Disregard for authority, Self-Centeredness, and Lack of Dependability has got 0.5. On the other hand, case attributes like Not Accepting Feedback, Stress, Disengagement, Personal Issues, and Disgruntlement are weighted

0.3. The highest weight was given for the attribute Addictions, which is 0.66. As there is an exact match between input values and value of case-based, equal local similarities are used for all case attributes.

Table 3 Managing the Case Structure in jCOLIBRI

Case Attributes	Data Type	Weight	Local Similarity
Disregard for Authority	Enum	0.5	Equal
Disgruntlement	Enum	0.3	Equal
Anger Management Issues	Enum	0.5	Equal
Confrontational Behavior	Enum	0.5	Equal
Disengagement	Enum	0.3	Equal
Not Accepting Criticism	Enum	0.3	Equal
Self-Centeredness	Enum	0.5	Equal
Stress	Enum	0.3	Equal
Performance	Enum	0.5	Equal
Lack of Dependability	Enum	0.5	Equal
Personal Issues	Enum	0.3	Equal
Absenteeism	Enum	0.5	Equal
Unexpected acquisition of wealth	Enum	0.5	Equal
Inattentiveness	Enum	0.5	Equal
Deception	Enum	0.5	Equal
Malingering	Enum	0.5	Equal
Addictions	Enum	0.66	Equal
Peer Pressure	Enum	0.5	Equal
Generosity	Enum	0.5	Equal
Outside working hours	Enum	0.5	Equal
Department	Enum	0.1	Equal
Fraud_Type	String	1.0	EqualStringingnrecase
Taken_Action	String	1.0	EqualStringingnrecase

5.2.4 Managing Connectors

After managing case structures on the system, like assigning weight and Similarity for the case attributes, manage data types; it's time to connect those managed cases with the stored cases. Connectors are objects that know how to access and retrieve cases from the storage media and return those cases to the CBR system in a uniform way. Therefore, connectors provide an abstraction mechanism that allows users to load cases from different storage sources in a transparent way. jCOLIBRI includes connectors that can work with plain text files, XML files, relational data bases and DLs systems. Here below figure 17 shows as the detail architecture of jCOLIBRI connector.

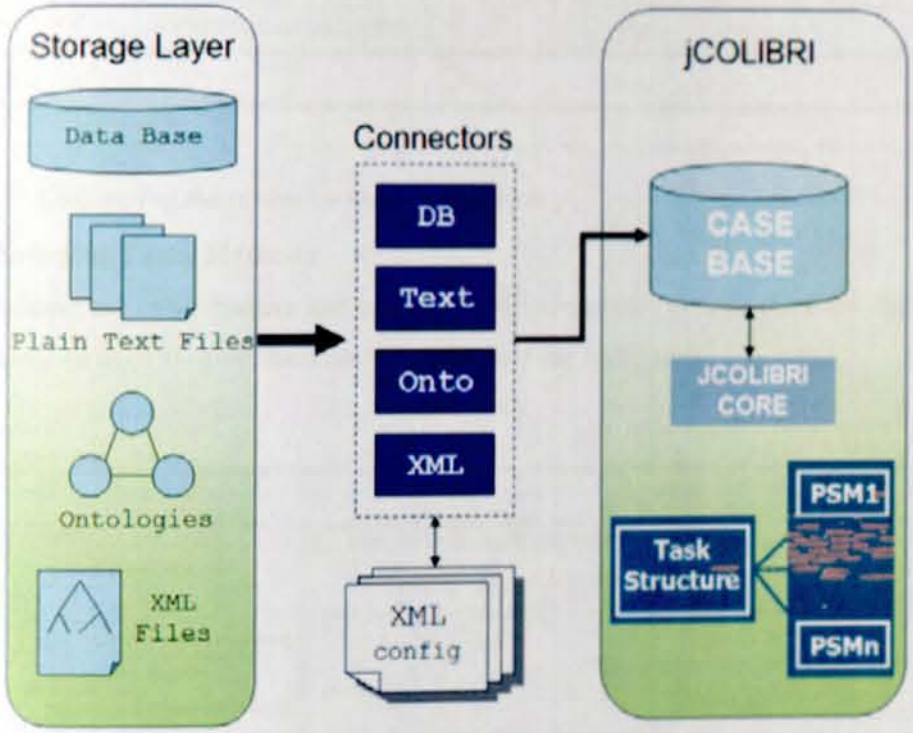


Figure 16 jCOLIBRI connector architecture

In our case as the cases are stored in SQL database format, the researcher used SQL database connector. As shown below on 18 the researcher has given the path of the case structure file saved in an xml format and all needed information about the database properties in which our cases are stored like, the database name, table name, and user.

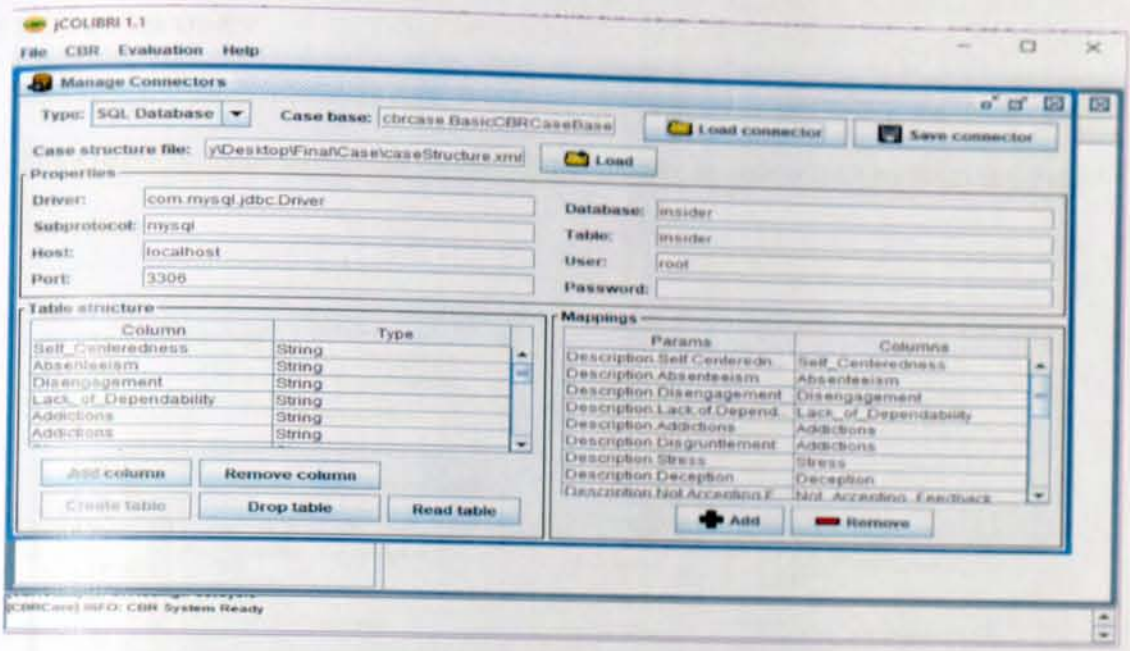


Figure 17 Configuring the connector with the case base

5.2.5 Managing Task/ Methods

After defining the case structure and configuring the connectors to store the Case Base of our application, we need to select the tasks and methods of our application.

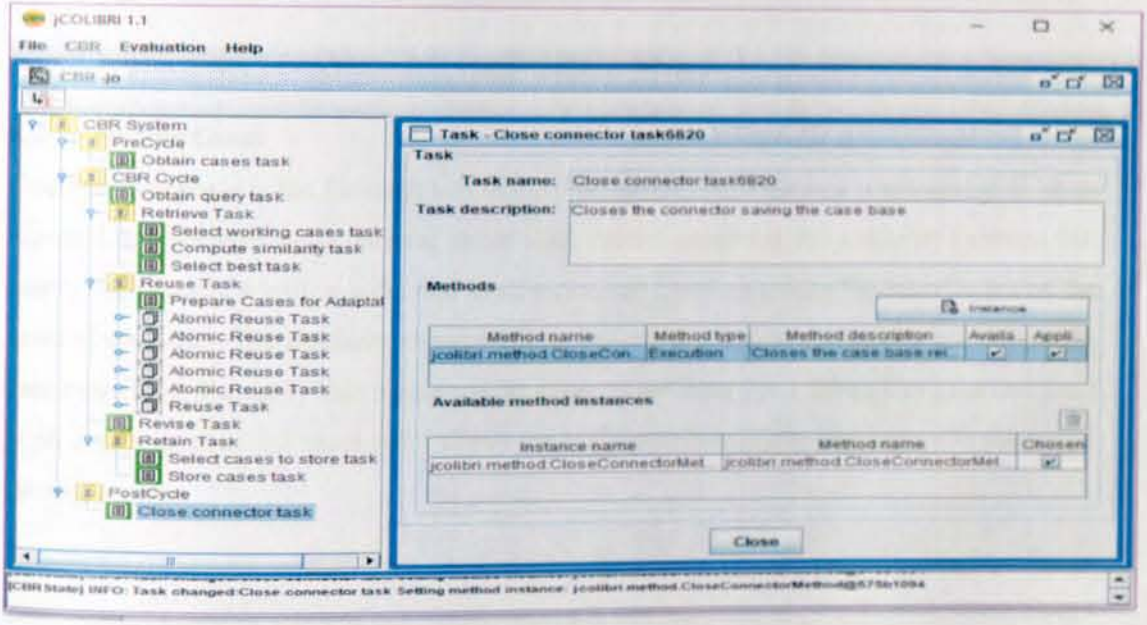


Figure 18 Managing Task and Methods

5.2.6 Define Query

Here after all configurations are done, it is time to give a query or new case to the system, so as shown below on figure 20 by using the query filled interface the user will fill the fields as per their observation.

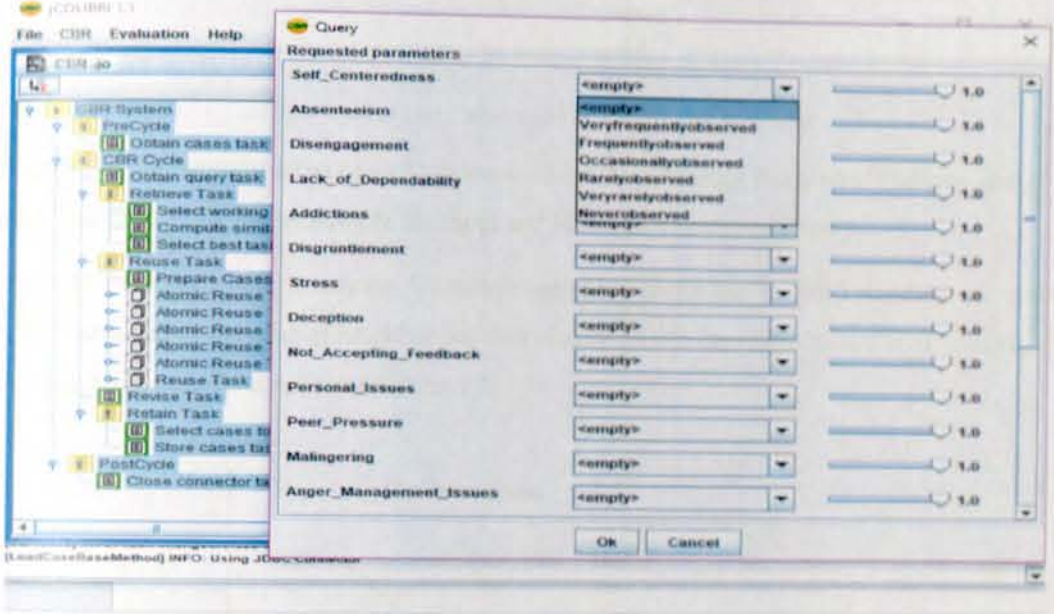


Figure 19 Query Field on jCOLIBRI

5.2.7Retrieve Cases

Case retrieval phase is the foremost step in the process of CBR. This step is considered to be an essential one because using retrieval phase CBR system computed the similarity between two cases. The existing situation is devised as new case and compare among the stored cases on the basis of similarity. The similarity computation will allow to retrieves one ormore cases from the case repository. Similarity values between the cases ranges from 0 to 1 where 0 reflects that there is no similarity in stored cases and 1 shows the 100% matching of the new case with the stored cases.

Nearest neighbor retrieval algorithm was used while the system retrieves cases from the knowledge base, nearest-neighbor retrieval is a simple approach that computes the similarity between stored cases and new input case based on weight features. A typical evaluation function is used to

compute nearest-neighbor matching Kolodner, 1993. Nearest-neighbor evaluation function as shown on figure 21 is explained below.

$$similarity(Case_I, Case_R) = \frac{\sum_{i=1}^{n} w_i \times sim(f_i^I, f_i^R)}{\sum_{i=1}^{n} w_i}$$

Figure 20 A nearest-neighbor evaluation function

Where w_i is the importance weight of a feature, *sim* is the similarity function of features, and f_i^I and f_i^R are the values for feature *i* in the input and retrieved cases respectively.

Figure 21 displays a simple scheme for nearest-neighbor matching. In this 2-dimensional space, *case3* is selected as the nearest neighbor because *similarity(NC, case3)*> *similarity(NC, case1)* and *similarity(NC, case3)*> *similarity(NC, case2)*.

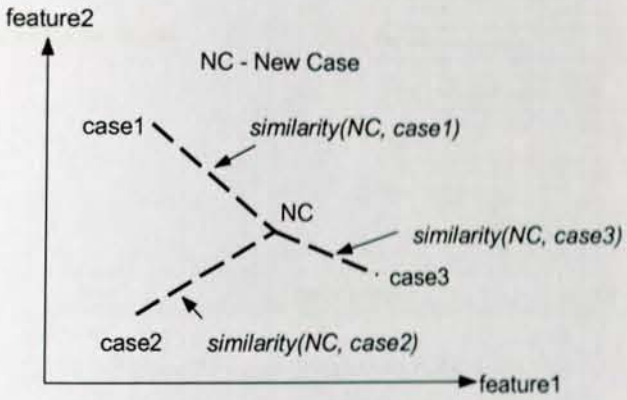


Figure 21 How to find the nearest neighbor of the new case NC

5.2.7 Revise Cases

Once the case is retrieved and adapted, the next step is revision stage. In this stage the adapted solution is being analyzed and verified for the accuracy and after the verification is done, it is offered as a validated solution for the new problem case. As shown below on figure 23 the user will go for investigation as per the solution given, and then after checking the correctness of the retrieved case any revision can be done before the stage retaining.

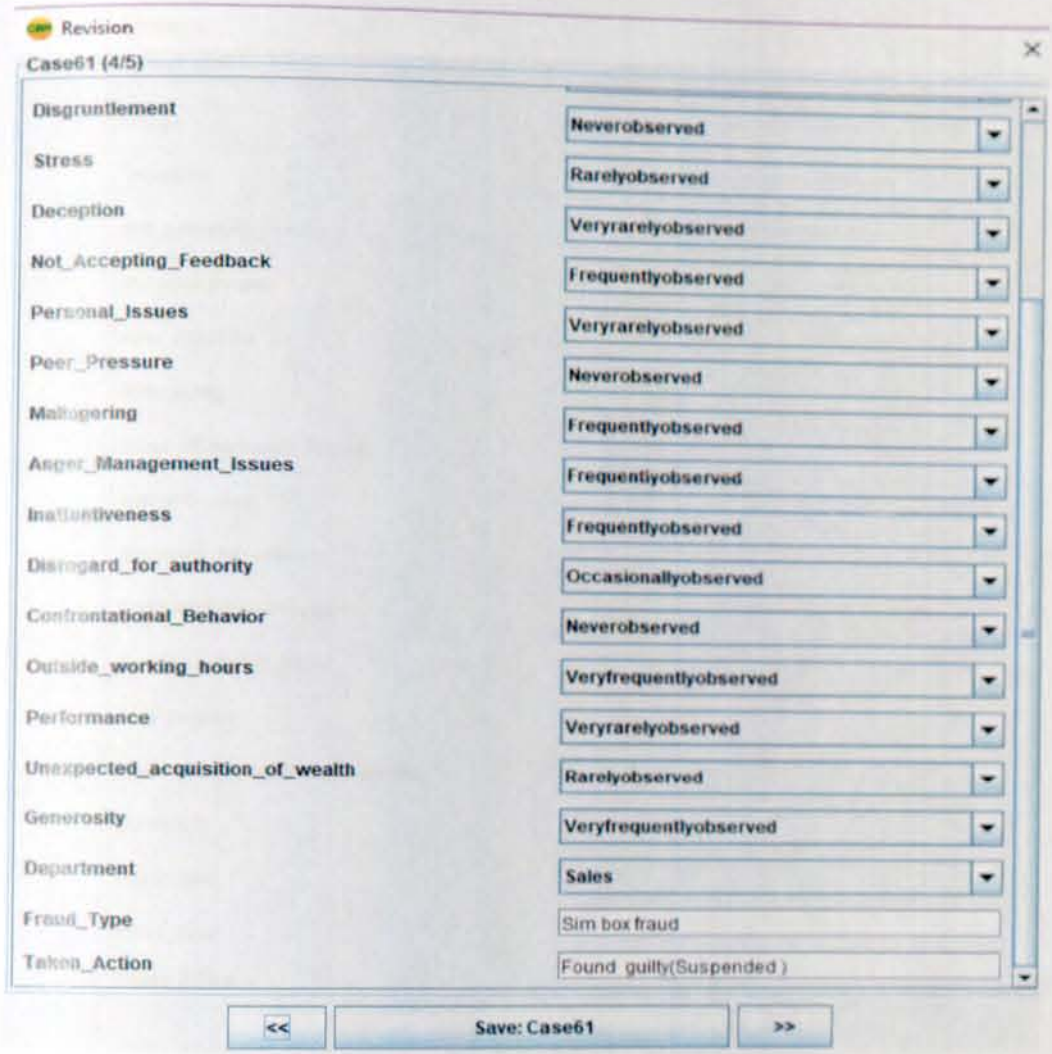


Figure 22 Case revision in jCOLIBRI

5.2.8 Case **Retain**

This is the final or last stage of CBR cycle and it is responsible for integrating new cases into the case repository or knowledge base for future utilization. So that the user is able to store the revised case in to the database for future use.

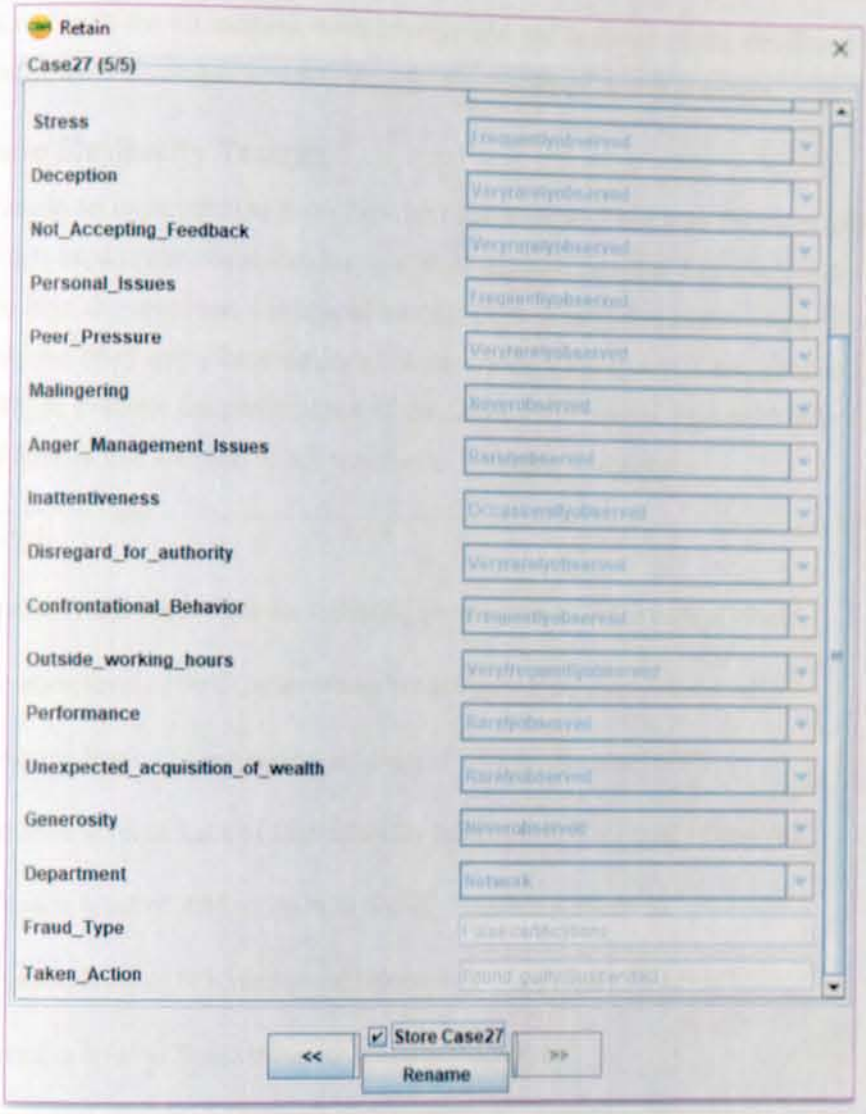


Figure 23 Case retention in jCOLIBRI

5.3 Testing and evaluating the prototype

Once the prototype is implemented, experimentations have to be conducted to test and evaluate the prototype. This chapter presents case similarity testing and evaluation of the prototype based on testing procedures quality model attribute tree to validate motive-centered queries. We setup concrete test cases based on example intelligence queries based on the scenario. After execution of these test cases, we evaluate the respective test results by means of quality and quantity

measures to check the correctness, completeness and performance of the developed prototype. Additionally, we will conduct usability tests for the developed search concepts.

5.3.1 Case Similarity Testing

We have made an experiment to know how new cases are matched with the cases from the case base. For this experiment, the researcher uses three input queries. The first query is directly taken from cases from the case base. The second query consists of modified attribute value from the case base, while the third query have empty attribute values. Each query is presented to the system individually to evaluate the performance of the similarity measures. Figure 25 below shows the sample of queries that are used in this experiment with their description.

User Query 1:

The observant employee has shown following observation level for each attribute

The observation level of Self-Centeredness behavior is" Very rarely observed".

The observation level of Absenteeism behavior is" Frequently observed".

The observation level of Lack of Dependability behavior is" Very rarely observed".

The observation level of Addictions behavior is" Frequently observed".

The observation level of Disgruntlement behavior is" Very rarely observed".

The observation level of Stress behavior is" Rarely observed".

The observation level of Deception behavior is" Frequently observed".

The observation level of Not Accepting Feedback behavior is" Rarely observed".

The observation level of Personal issues behavior is" Very frequently observed".

The observation level of Peer Pressure is" Frequently observed".

The observation level of Malingering behavior is" Frequently observed".

The observation level of Anger management issue behavior is" Frequently observed".

The observation level of Inattentiveness behavior is" Frequently observed".

The observation level of Disregard for authority behavior is" Occasionally observed".

The observation level of Confrontational behavior is" Occasionally observed".

The observation level of Outside working hours' behavior is" Very frequently observed".

The observation level of Performance behavior is" Rarely observed".

The observation level of Unexpected acquisition of wealth behavior is" Very frequently observed".

The observation level of Generosity behavior is "Rarely observed".

The observant employee is working for Sales department of Ethio telecom.

Figure 24 Input values of the requested parameters in jCOLIBRI1.1

As shown below on table 4 user query 1 has exactly matched case 5 and their similarity is 1.0, whereas user query 2 has 1 attribute value modification and the result shows their similarity goes to 0.9. The third user query has empty input, so there is no any related case and their similarity is 0.0. The results show that case similarity is working and performing well.

Table 4 Sample of Query for Case Similarity Testing and their Corresponding Similarity

Answered Query	Cases	Similarity [0 - 1]
User Query 1	Case 5	1.0
User Query 2	Case 5	0.904
User Query 3	Null	0.0

5.3.2 System Performance Testing

So, in order to assure the CBR system meets the requirement it is developed the system has to be tested and evaluated. The researcher has used 28 testing data set for the seven cases.

Table 5 Confusion matrix for evaluation of the case base system

	Fraud Cases	Benefit related	Data theft related fraud	False certifications	Inventory Theft	Sim box fraud	SIM card related	VAS related fraud	Total
Test Case	Benefit related	4	0	0	0	0	0	0	3
	Data theft related fraud	0	3	0	0	0	1	0	3
	False certifications	0	0	3	0	0	0	1	3
	Inventory Theft	0	1	0	3	0	0	0	3
	Sim box fraud	0	0	0	0	4	0	0	3
	SIM card related	0	0	1	0	0	3	0	3
	VAS related fraud	1	0	0	0	0	0	3	3
	Total	5	4	4	3	4	4	4	28

Table 6 Performance evaluation based on Precision, Recall and F-measure

Cases	n(truth)	n(classified)	Accuracy	Precision	Recall	F1 Score
Benefit related	5	4	96.43%	1.0	0.80	0.89
Data theft related fraud	4	4	92.86%	0.75	0.75	0.75
False certifications	4	4	92.86%	0.75	0.75	0.75
Inventory Theft	3	4	96.43%	0.75	1.0	0.86
Sim box fraud	4	4	100%	1.0	1.0	1.0
SIM card related	4	4	92.86%	0.75	0.75	0.75
VAS related fraud	4	4	92.86%	0.75	0.75	0.75

The overall evaluation result shows that the case-based reasoning prototype for insider threat mitigation is very encouraging as the retrieval performance of the prototype registers 8an average value of 82.14% precision and 82.85 % recall with average accuracy of 94.90%.

5.3.3 User Acceptance Testing

User acceptance testing is the process in which the actual system users test the system to make sure it can handle required tasks in real world scenario. Ten users were selected from those who participated in the knowledge accusation process. The researcher has given detail explanation how the CBR system works before testing it.

For the evaluation of the user acceptance testing, different researchers used different evaluation criteria. On our work we have customized and adapted evaluation criteria suggested by Dawit (2015), Alemu (2010), and Seblewongel based on the ISO standard 9126, as shown below on figure 25 below.

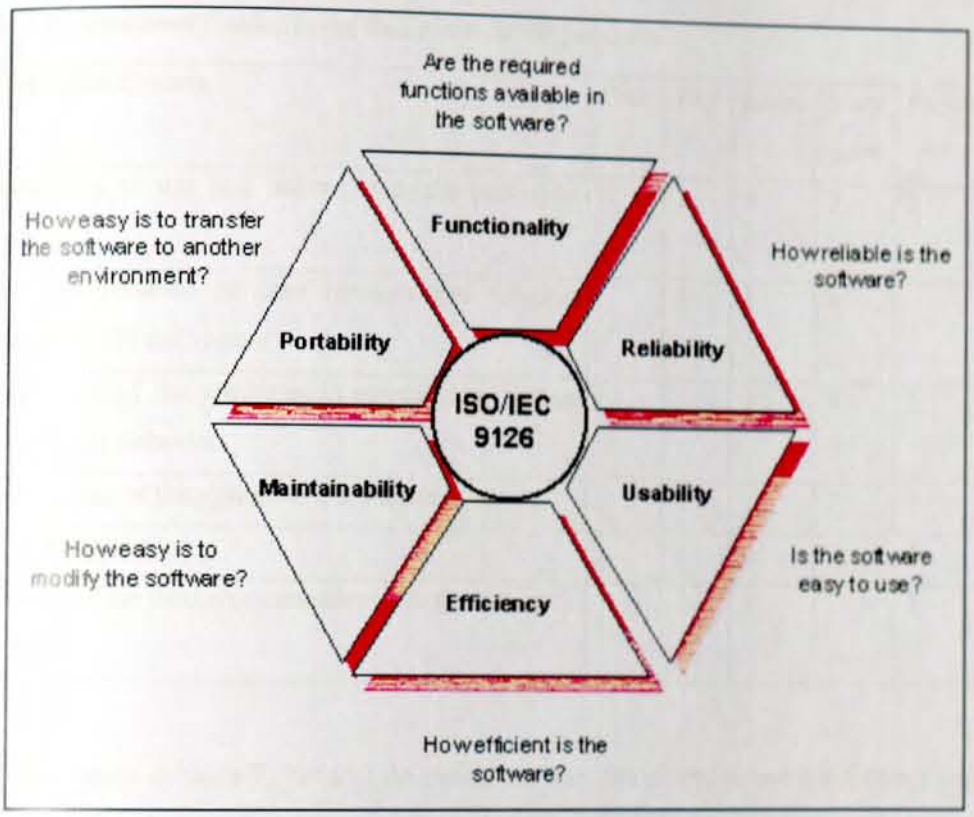


Figure 25 The six ISO 9126 quality characteristics of a software

Ten selected users evaluate the CBR system by using the following criteria.

- ✓ Simplicity to use and interact with the prototype system
- ✓ The performance of case revision and solution adaptation
- ✓ The ability of the prototype system in making right recommendations
- ✓ Importance of the system in the domain area
- ✓ Efficiency in time
- ✓ Fitness of the final recommendation to the new case at hand

Table 7 Performance Evaluation of the System by the end users

No.	Evaluation Criteria	Poor	Fair	Good	Very good	Excellent	Average
1	Simplicity to use and interact with the prototype system		1	4	3	2	3.8
2	The performance of case revision and solution adaptation of the system		2	4	4		3.2
3	Relevance of the attributes in representing human observable behavior			2	5	3	4.1
4	Importance of the system in the domain area				3	7	4.7
5	Efficiency in time				2	8	4.8
6	Fitness of the final recommendation to the new case at hand			1	7	2	4.1

As shown above on table 7, 70 % of the evaluators rate 'Simplicity to use and interact with the prototype system' as good and very good, while 10% and 20% of them respectively rate as fair and excellent. For the criteria 'performance of case revision and solution adaptation of the system' equal 40% good, and 40% very good rate is registered, and 20% of the evaluators rated as fair. On the other hand, 50%, 30%, and 20% of the evaluators rated very good, excellent and good respectively for the criteria 'relevance of the attributes. 'Importance of the system in the domain area' was the other criteria being evaluated by the evaluators, and rated as 70% excellent and 30% very good, which has a close result with the criteria 'efficiency in time' with 80% excellent and 20% very good result. The last evaluation criteria were the 'fitness of the final recommendation to the new case at hand', which has 70% very good, 20% excellent, and 10% good rating.

Average of 4.12 which means a very good result is obtained from the final work, and in which the result shows that the system has an encouraging user acceptance.

5.4 Discussion of the Result

As case similarity test has been done in order to check wither case similarity is working well or not by giving the system 3 queries, the result shows that as the cases are more similar to the stored one the result can be at the highest 1.0 and at the reverse as their similarity are much different the result can go down to 0.0. Here it shows us clearly that as queries get more similar cases from the case base, better similarity result can be registered.

The system performance test result meet 82.14% precision and 82.85 % recall with average accuracy of 94.90%. The test was performed using 28 testing data sets with respect to 70 learning datasets stored in the knowledge base. Though the results are encouraging, the researcher believe that the inconsistency characteristics of those human observable behaviors are the main reason for not meeting over all 100% accuracy.

On average very good grade was registered from User evaluation based on the criteria's simplicity to use and interact with the prototype system, the performance of case revision and solution adaptation of the system, Relevance of the attributes in representing human observable behavior, Importance of the system in the domain area, efficiency in time, and fitness of the final recommendation to the new case at hand.

Generally, the case-based reasoning approach in designing insider threats behavior identification system meets an encouraging result on its overall performance test and user evaluations.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 CONCLUSION

On this research work the researcher has made an attempt on applying case-based reasoning system in depicting employee's behavior towards potential frauds to be committed by identifying at risk employees and recommending possible related fraud types to be committed, by using human observable behaviors. The required knowledge was acquired from two group of experts, seven previously investigated insider cases, document analysis and other relevant information through a

six-point Likert scale questionnaire survey. Investigated cases were gathered from Ethio telecom legal department and information science department. The domain experts were selected from Addis Ababa University, FDRE attorney general and self-employed personnel, using purposive sampling. The researcher came across with eight new human behavior indicators, which can be used as spring board to conduct further research works on the domain area, and this study shows that we can identify insiders objectively by using case-based reasoning, based on identified observable behaviors.

For modeling purpose of the acquired knowledge, hierarchical tree modeling technique were used. Attributes that are relevant and have direct impact on the decision were selected and the case structure formulated. Eight new human behavior indicators were

The case based was developed using JCOLIBRI1.1. The system has the capability in retrieving, reusing, revising, and retaining new cases. And here nearest neighbor retrieval algorithm was used while the system retrieves cases from the knowledge base. In order to assure the CBR system has meet the requirement needed, evaluation was conducted on both the system performance and user acceptance test.

The overall evaluation result shows that the case-based reasoning prototype for insider threat mitigation is very encouraging as the retrieval performance of the prototype registers an average value of 82.14% precision and 82.85 % recall with average accuracy of 94.90%. And also, the system has registered an average grade of "very good" in user satisfaction test result.

In general, the work has achieved its objective by developing the expected prototype with an encouraging system performance and user acceptance test result on designing knowledge-based system for insider threat mitigation using human observable behaviors.

6.2 RECOMMENDATION

Though the study has met its objectives by using Case Based Reasoning approach in designing the knowledge base for depicting employee's behavior towards potential frauds to be committed, the researcher believe that other researchers are supposed to enrich the work on the following aspects.

- The researcher recommends other organizations to turn their face to intelligence-based insider's identification mechanism.
- As insiders are the most dangerous threats of an organization, giving high attention only for external threats will be valueless. So, the researchers recommend organizations to do a lot on insiders' threats.
- Higher officials and security personnel's have to give attention on human observable behaviors, rather than only focusing on deploying technology to control insiders.

6.3 Future Work

- As the study is limited to develop a prototype knowledge-based system for the purpose of identifying insider threats behavior, and doesn't give punishment decision for the new cases, the researchers believe that further researches can be conducted by incorporating company rule and regulation and integrating with rule-based reasoning.
- Seven insider threats gathered from Ethio telecom have been used in this study. But, if the number of cases increased in the case base, by extending the scope to other organizations, then performance of the system can also increase. Therefore, it is recommended that extension of this work by adding more insider threat cases in the case base to increase the performance of the prototype system.

References

1. Aamodt, A. and Plaza, E, 1994. Case based reasoning: Foundational issues, methodology variations and system approaches. AICom Vol. 7(Issue 1), pp. 39.
2. AIAI CBR Shell. Retrieved from http://www.aiai.ed.ac.uk/project/cbr/CBRDistrib .
3. Alemu Jorgi, 2010. A Case-Based Approach for Designing Knowledge-Based System for AIDS Resource Center (ARC): The Case of Warmline Clinician Consultation Service. Msc Thesis, Addis Ababa University, Ethiopia.
4. Ambrose, ML, MA Seabright, and M Schminke. 2002, "Sabotage in the Workplace: The Role of Organizational Injustice." Organizational Behavior and Human Decision Processes 89:947-65.
5. Aronson J.E. and Turban E., 2004. Decision Support Systems and Intelligent Systems, New Delhi: Printice-Hall of India.
6. B. D´ıaz-Agudo, P.A. Gonz´alez-Calero, 2000. An architecture for knowledge intensive CBR systems", Advances in Case-Based Reasoning, EWCBR'00, Springer-Verlag, Berlin, Heidelberg, New York.
7. B.G. Buchanan and E.H. Shortliffe (eds.). 1985. Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project, Reading, MA: Addison-Wesley.
8. Burroughs, SM, and LR James. 2005, "Advancing the Assessment of Dispositional Aggressiveness through Conditional Reasoning." in Counterproductive Work Behavior: Investigations of Actors and Targets, eds. S Fox and PE Spector, pp. 127-50. American Psychological Association, Washington, DC.
9. Burroughs, SM, and LR James. 2005, "Advancing the Assessment of Dispositional Aggressiveness through Conditional Reasoning." in Counterproductive Work Behavior: Investigations of Actors and Targets, eds. S Fox and PE Spector, pp. 127-50. American Psychological Association, Washington, DC.
10. C. Colwill, "Human factors in information security: The insider threat who can you trust these days?" Information Security Technical Report, vol. 14, no. 4, pp. 186–196, 2009.
11. Cappelli, D, et al. 2009, Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1. Technical, Carnegie-Mellon University. Software Engineering Institute. CERT Coordination Center.

12. Case-Based Reasoning System and Artificial Neural Networks: A Review Daqing Chen and Phillip Burrell Knowledge-Based Systems Centre, School of Computing, Information System and Mathematics, South Bank University, London, UK.
13. CERT Insider Threat Team, 2014. "Unintentional Insider Threats: Social Engineering,", Carnegie Mellon Univ, vol.CMU/SEI-20.
14. Chabris C.F., 1989. Artificial intelligence and Turbo Pascal, New Delhi: Galgotia Publications prv.ltd, India.
15. Clancey, WJ, 1985. "Heuristic classification". Artificial Intelligence 27 289-350.
16. Costa, P.C.G., Laskey, K.B., Revankar, M., Mirza, S., Alghamdi, G., Barbará, D., Shackelford, T. & Wright, E.J., 2005. DTB Project : A Behavioral Model for Detecting Insider Threats. In International Conference on Intelligence Analysis. McLean, VA: MITRE Corporation.
17. Creswell, J. W. 1994 . Research Design: Qualitative and Quantitative Approaches. Thousand Oaks, CA: SAGE.
18. D. Cappelli, A. P. Moore, and R. Trzeciak, 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes, 1st ed. Addison-Wesley Professional.
19. Dawit Hassen, 2015. Integrating Descriptive Modelling with Case Based Reasoning in Network Intrusion Detection. Msc Thesis, Addis Ababa University, Ethiopia.
20. Department of Trade & Industry, UK. Falkeneheimer, B, Forbus, KD and Gentner, D, 1986. "The structure mapping engine". In: Proceedings Sixth National Conference on Artificial Intelligence, Philadelphia, PA.
21. Dhillon, G., Moores, S, 2001.: Computer Crimes: theorizing about the enemy within. Comput.Secur. 20(8), 715–723.
22. E. D. Shaw and H. V. Stock, 2011. "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall," Symantec, Tech. Rep.
23. Eisenhardt, K, 1989. Building theories from case study research. Academy of Management Review, 14(4), 532-550.
24. Greitzer, F.L., Paulson, P.R., Kangas, L.J., Franklin, L.R., Edgar, T.W. & Frincke, D.A., 2009. Predictive Modeling for Insider Threat Mitigation.

25. Group for Artificial Intelligence Applications. Department of Software Engineering and Artificial Intelligence. Universidad Complutense de Madrid. jCOLIBRI CBR. Retrieved January 11, 2019.
26. Hamin, Z., 2000. Insider Cyber-threats: Problems and Perspectives. International Review of Law, Computers & Technology, 14(1), pp.105–113.
27. ITU (2014, September 20) Cybersecurity. ITU News. Retrieved from https://www.itu.int.
28. J. Hunker and C. W. Probst, "Insiders and insider threats – an overview of definitions and mitigation techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 1, pp. 4–27.
29. J. Kolodner, Case-Based Reasoning. San Mateo, CA: Morgan Kaufmann Publishers, 1993.
30. K. J. Hammond, Case-Based Planning., Vol. 1, Can Diego, CA: Academic Press Inc., 1989.
31. Kjaerland, M, 2006, A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers and Security, 25:522-538.
32. Kolodner, J, 1993, Case based reasoning Morgan Kaufmann.
33. Kramer, LA, RJ Heuer, Jr., and KS Crawford. 2005, Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage. Technical Rpt. TR 05-10, Defense Personnel Security Research Center, Monterey, CA.
34. Leake, B. 1995. Case-Based Reasoning: Issues, Methods and Technology. A Tutorial for the First International Conference on Case-Based Reasoning.
35. M. Sasikumar, "Case Based Reasoning," NCST Technical Report, National Center for Software technology, NCST.
36. Mack, N., Kathleen, C. Macqueen, M., Guest, G. and Namey, E. (2005) Qualitative Research Methods: A Data Collector's Field Guide. 1st ed. USA.
37. McGarry, M, 2006. Engines for education: Case-based reasoning in the real world (http://www.engines4ed.org/hyperbook/nodes/NODE-195-pg.html). (Last Accessed: May 24th 2006).
38. Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M. & Johnston, K., 2014. A Descriptive Literature Review and Classification of Insider Threat Research. In Proceedings of Informing Science & IT Education Conference (InSITE). pp. 211–223.

39. Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S, 2008. "A Design Science Research Methodology for Information Systems Research." Journal of Management Information Systems, 24(3), 34.
40. PwC (2014) A worldwide study on The Global State of Information Security Survey, CIO magazine, and CSO magazine.
41. Reid, G., 1985. "Knowledge-Based Systems Concepts, Techniques, Examples" (PDF). reidgsmith.com. Schlumberger-Doll Research. Retrieved January 11, 2019.
42. Ross, B.H (1989): Some psychological results on case-based reasoning. Case-Based Reasoning Workshop, DARPA 1989. Pensacola Beach. Morgan Kaufmann. pp. 144-147).
43. Russell, Stuart J.; Norvig, Peter (2009). Artificial Intelligence: A Modern Approach (3rd ed.). Upper Saddle River, New Jersey: Prentice Hall.
44. Schank, R, 1982. Dynamic memory; a theory of reminding and learning in computers and people. Cambridge University Press.
45. Seblewongel Esseynew, 2011. Prototype Knowledge Based System for Anxiety Mental Disorder Diagnosis. Msc Thesis, Addis Ababa University, Ethiopia.
46. Shaw, E.D., Post J., Ruby, K, 1999. Inside the mind of the insider. Security Management, pp. 34-44.
47. Shaw, ED, LF Fischer, and AE Rose. 2009, Insider Risk Evaluation and Audit. Technical Rpt. TR 09-02, Defense Personnel Security Research Center, Monterey, CA.
48. Shropshire, J. 2009, "A Canonical Analysis of Intentional Information Security Breaches by Insiders." Information Management and Computer Security 17:296-310.
49. Verizon and U.S. Secret Service. 2010, "2010 Data Breach Investigations Report."
50. Warkentin, M.E., Willison, R, 2009. Behavioral and policy issues in information systems security: The insider threat. Eur. J. Inf. Syst. 18(2), 101–105.
51. Watson, I. and Marir, F. 1994, Case-based reasoning: A review. The Knowledge Engineering Review Vol. 9(Issue 4).
52. Watters, P. A, 2012. McCrombie, S., Layton, R., Pieprzyk, J.: Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP), Journal of Money Laun-dering Control, Vol. 15 (4): 430-441, Emerald Group Publishing.

APPENDIX I: QUESTIONNAIRE

Date01/03/2019

Dear Participant:

My name is Yohanes Halefom Abadi and I am a post graduate student at Addis Ababa University. For my final thesis, I am examining how often the selected attributes on this survey were observed on the insider that was terminated before, under your supervision. Because you are working for Ethio telecom on managerial position , I am inviting you to participate in this research study by completing the attached surveys.

There is no compensation for responding nor is there any known risk. In order to ensure that all information will remain confidential, please *do not* include your name. Copies of the thesis will be provided to my Addis Ababa University advisor and to Addis Ababa University School of Information Science. If you choose to participate in this thesis, please answer all questions as honestly as possible and return the completed questionnaires promptly in person. Participation is strictly voluntary and you may refuse to participate at any time.

Thank you for taking the time to assist me in my educational endeavors. The data collected will provide useful information regarding the work on selecting observable behavior of humans, which to be used to identify employees-at-risk before any fraud activities happen to the company.. Completion and return of the questionnaire will indicate your willingness to participate in this study. If you require additional information or have questions, please don't hesitate to contact me at the number listed below.

Sincerely,

Yohanes Halefom

+251 930800244 yhalefom@ymail.com

Million Meshesha (PhD)

meshe84@gmail.com

The following items describe attributes about observable behavior of humans, which are intended to be used to identify employees-at-risk before any fraud activities happen to the company. Rate your observations according to the fraud case happened under your supervision, with the following statements by putting check mark (x) in the box provided. For any additional observed indicator(s) other than the below stated indicators please put it on the provided empty rows at the end of the survey and please follow the same instruction while rating.

Sim box related fraud							
Indicator	**Description of indicator**	1 Very Frequently observed	2 Frequently observed	3 Occasionally observed	4 Rarely observed	5 Very Rarely observed	6 Never Observed
Disregard for Authority	The employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.						
Disgruntlement	Employee is observed to be dissatisfied in current position; shows chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid or undervalued; may have a poor fit with current job.						
Not Accepting Feedback	The employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message						
Anger Management	The employee often allows anger to get pent up inside; employee observed to have trouble managing lingering emotional feelings of anger or rage; hold strong grudges.						

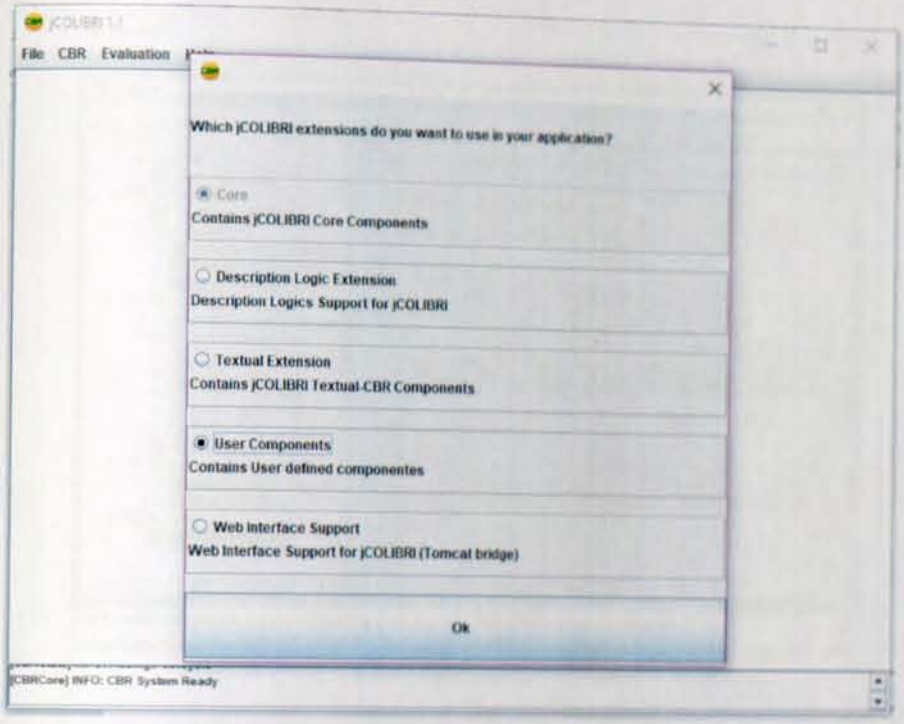
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoids meetings.						
Performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.						
Stress	The employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.						
Confrontational Behavior	Employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.						
Personal Issues	Employee has difficulty keeping personal issues separate from work, and these issues interfere with work.						
Self-Centeredness	The employee disregards needs or wishes of others, concerned primarily with own interests and welfare.						
Lack of Dependability	Employee is unable to keep commitments /promises; unworthy of trust.						
Absenteeism	Employee has exhibited chronic unexplained absenteeism.						
Unexpected acquisition of wealth	Employee has exhibited with unusual wealth with their income. Such as buying new car, wearing brand materials, buying house and the like...						

Inattentiveness	Employee exhibits impulsive, amoral, uncontrolled and detached from normal relationships.						
Deception	Employee told lies, said nasty things, blackmailed someone or told about other peoples that were not true.						
Malingering	Employee deliberately falsifying the symptoms of illness for secondary gain, exaggeration of existing depressive symptoms or failure to make enough effort in a cognitive task.						
Addictions	Employee exhibited being addicted on different on different types of addictions. Like drug, alcohol, chat and the likes.						
Peer Pressure	The employee has a feeling that one must do the same things as other people of one's age and social group in order to be liked or respected by them.						
Generosity	The employee exhibited showing a readiness to give more of something, especially money, than is strictly necessary or expected.						
Outside working hours	The employee is exhibited coming to office outside the company's working hours.						

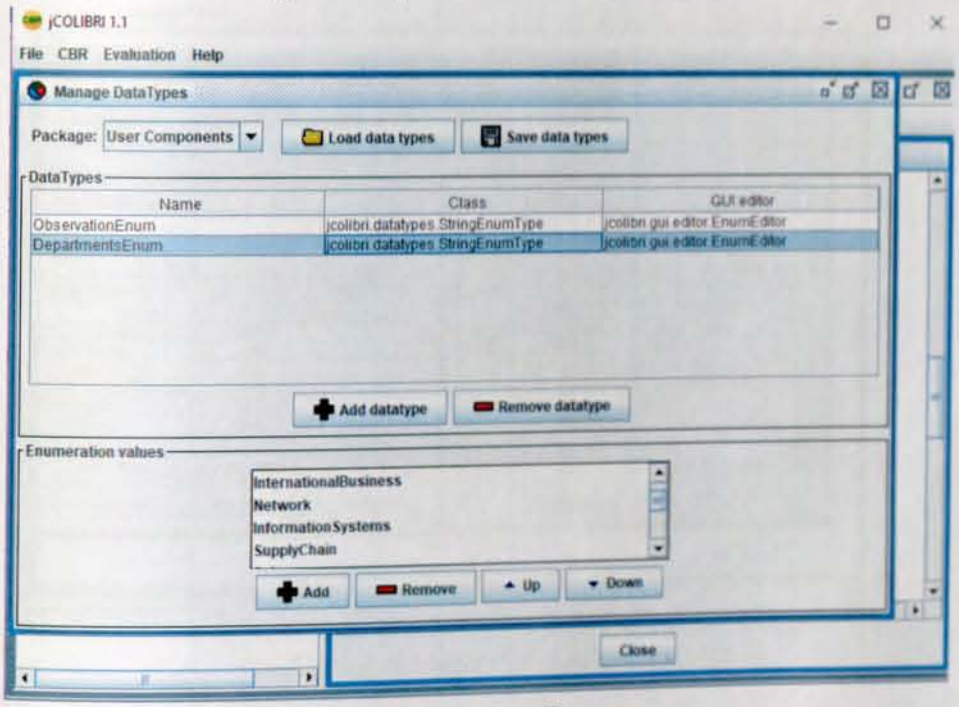
Appendix II: jCOLIBRI 1.1

The main window of the jCOLIBRI

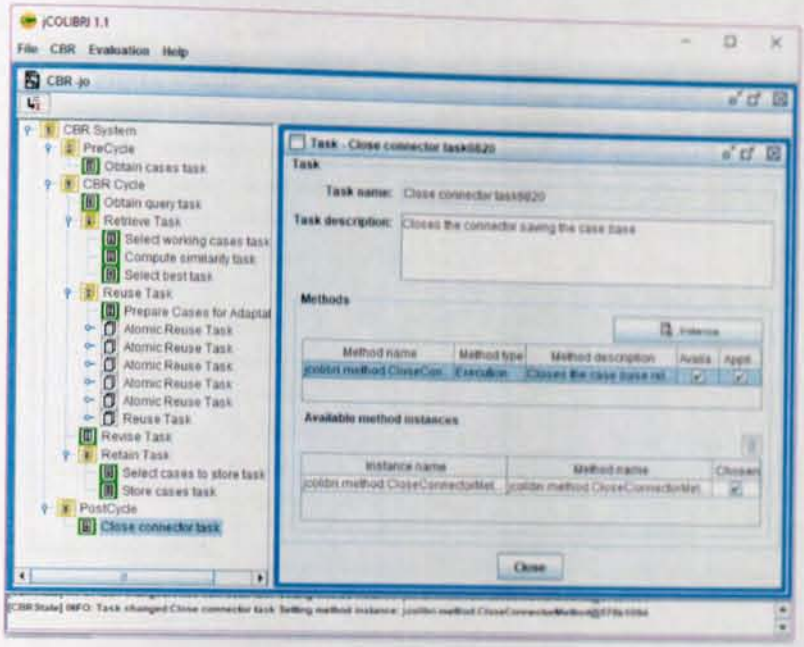
Window for Creating a new application of the jCOLIBRI



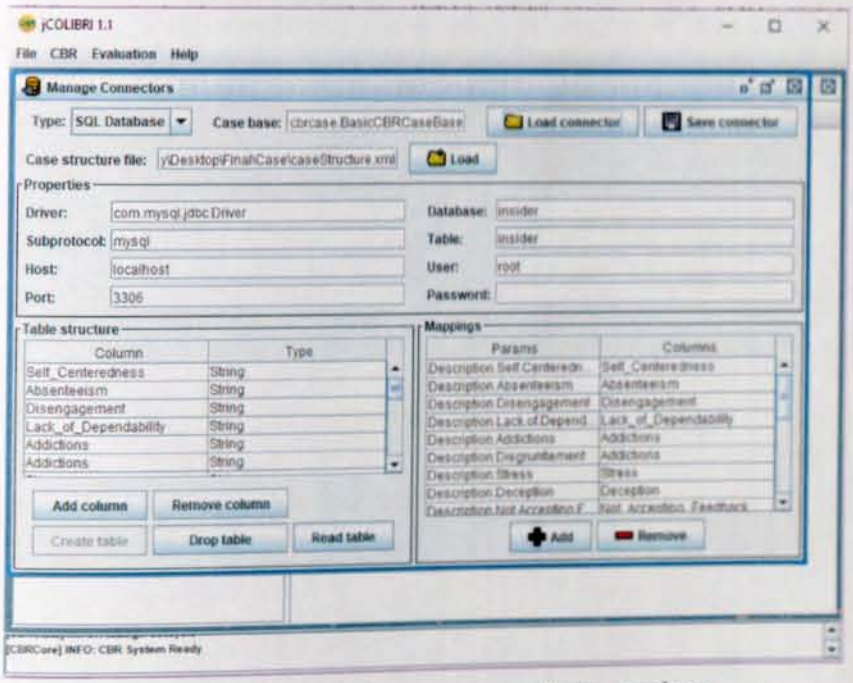
Selecting user component as an extension on jCOLIBRI



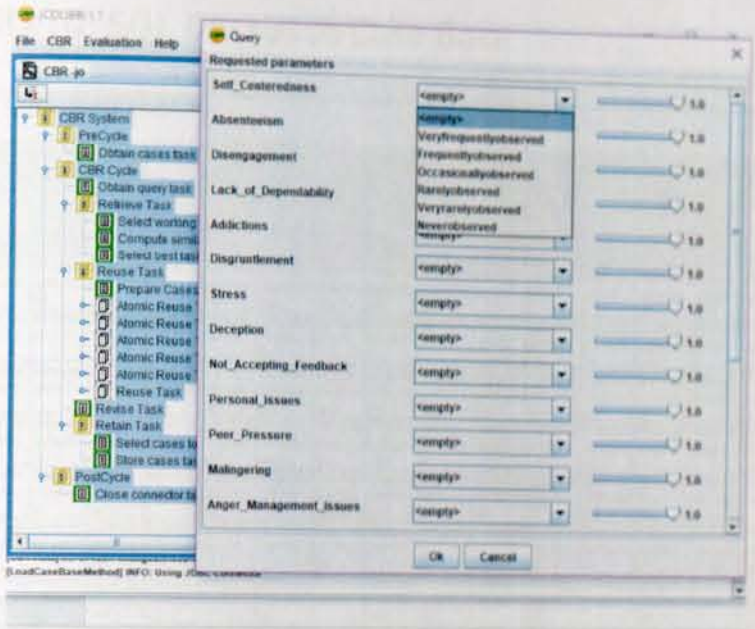
Managing Data Types



Managing Task and Methods



Configuring the connector with the case base



Query field interface

Appendix III: SQL Database Case Base

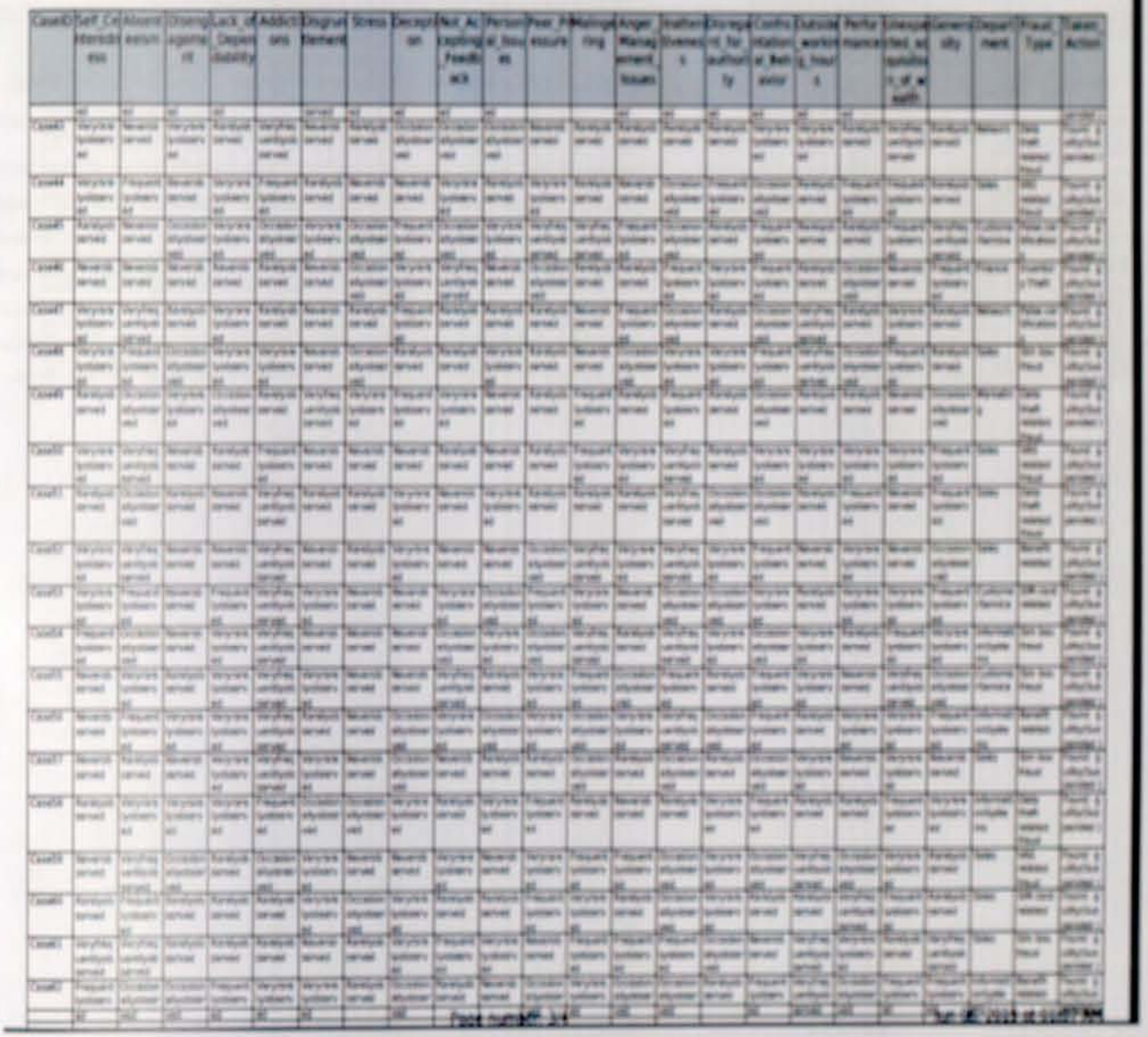
Database: insider, Table: insider, Purpose: Dumping data

CaseID	Self_Centeredness	Absenteeism	Disengagement	Lack_of_Dependability	Addictions	Disgruntlement	Stress	Deception	Not_Accepting_Feedback	Personal_Issues	Peer_Pressure	Maliciousness	Anger_Management_Issues	Inattentiveness	Disregard_for_authority	Confrontational_Behavior	Outside_working_hours	Performance	Unexpected_acquisition_of_wealth	Generosity	Department	Fraud_Type	Taken_Action
Case1	Very rarely observed	Very rarely observed	Very rarely observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Occasionally observed	Occasionally observed	Very rarely observed	Very rarely observed	Occasionally observed	Rarely observed	Rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Rarely observed	Occasionally observed	Rarely observed	Sales	SIM card related	Found guilty(Sued penalized)
Case2	Very rarely observed	Never observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Rarely observed	Never observed	Very rarely observed	Rarely observed	Rarely observed	Rarely observed	Never observed	Rarely observed	Very rarely observed	Occasionally observed	Rarely observed	Frequently observed	Very rarely observed	Rarely observed	Sales	Benefit related	Found guilty(Sued penalized)
Case3	Rarely observed	Very rarely observed	Occasionally observed	Very rarely observed	Rarely observed	Very rarely observed	Occasionally observed	Frequently observed	Occasionally observed	Occasionally observed	Frequently observed	Frequently observed	Frequently observed	Occasionally observed	Occasionally observed	Frequently observed	Rarely observed	Rarely observed	Occasionally observed	Verified identity served	Customer Service	SIM card related	Found guilty(Sued penalized)
Case4	Never observed	Never observed	Never observed	Very rarely observed	Very rarely observed	Rarely observed	Occasionally observed	Very rarely observed	Verified identity observed	Very rarely observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Frequently observed	Frequently observed	Rarely observed	Occasionally observed	Occasionally observed	Frequently observed	Information Security	Benefit related	Found guilty(Sued penalized)
Case5	Very rarely observed	Frequently observed	Rarely observed	Very rarely observed	Frequently observed	Very rarely observed	Rarely observed	Frequently observed	Rarely observed	Verified identity served	Frequently observed	Frequently observed	Frequently observed	Frequently observed	Occasionally observed	Occasionally observed	Verified identity served	Rarely observed	Verified identity served	Rarely observed	Sales	SIM card related	Found guilty(Sued penalized)
Case6	Very rarely observed	Frequently observed	Occasionally observed	Rarely observed	Rarely observed	Very rarely observed	Occasionally observed	Rarely observed	Rarely observed	Occasionally observed	Never observed	Very rarely observed	Occasionally observed	Frequently observed	Frequently observed	Frequently observed	Verified identity served	Occasionally observed	Frequently observed	Rarely observed	Information Security	VAS related fraud	Found guilty(Sued penalized)
Case7	Rarely observed	Very rarely observed	Very rarely observed	Very rarely observed	Very rarely observed	Occasionally observed	Very rarely observed	Frequently observed	Very rarely observed	Rarely observed	Occasionally observed	Very rarely observed	Rarely observed	Frequently observed	Rarely observed	Occasionally observed	Rarely observed	Rarely observed	Frequently observed	Occasionally observed	Customer Service	SIM box fraud	Found guilty(Sued penalized)
Case8	Very rarely observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Rarely observed	Never observed	Never observed	Rarely observed	Very rarely observed	Frequently observed	Very rarely observed	Very rarely observed	Never observed	Very rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Never observed	Frequently observed	Sales	SIM box fraud	Found guilty(Sued penalized)
Case9	Rarely observed	Occasionally observed	Rarely observed	Never observed	Very rarely observed	Never observed	Rarely observed	Very rarely observed	Never observed	Never observed	Very rarely observed	Occasionally observed	Rarely observed	Occasionally observed	Very rarely observed	Occasionally observed	Rarely observed	Frequently observed	Very rarely observed	Frequently observed	Information Security	Benefit related	Found guilty(Sued penalized)
Case10	Very rarely observed	Never observed	Never observed	Very rarely observed	Rarely observed	Never observed	Rarely observed	Very rarely observed	Never observed	Rarely observed	Never observed	Rarely observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Never observed	Very rarely observed	Frequently observed	Occasionally observed	Sales	SIM box fraud	Found guilty(Sued penalized)
Case11	Very rarely observed	Never observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Never observed	Never observed	Very rarely observed	Never observed	Never observed	Never observed	Never observed	Very rarely observed	Never observed	Rarely observed	Very rarely observed	Never observed	Frequently observed	Sales	Inventory Theft	Found guilty(Sued penalized)
Case12	Frequently observed	Never observed	Never observed	Occasionally observed	Never observed	Never observed	Never observed	Never observed	Frequently observed	Never observed	Never observed	Very rarely observed	Rarely observed	Never observed	Frequently observed	Never observed	Very rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Sales	SIM card related	Found guilty(Sued penalized)
Case13	Never observed	Never observed	Rarely observed	Rarely observed	Never observed	Rarely observed	Never observed	Never observed	Rarely observed	Never observed	Never observed	Very rarely observed	Occasionally observed	Never observed	Occasionally observed	Never observed	Very rarely observed	Never observed	Never observed	Occasionally observed	Fleet and Facilities	Inventory Theft	Found guilty(Sued penalized)
Case14	Never observed	Never observed	Very rarely observed	Never observed	Never observed	Occasionally observed	Never observed	Never observed	Rarely observed	Very rarely observed	Never observed	Very rarely observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Rarely observed	Very rarely observed	Never observed	Frequently observed	Customer Service	SIM card related	Found guilty(Sued penalized)
Case15	Never observed	Very rarely observed	Never observed	Never observed	Never observed	Very rarely observed	Never observed	Never observed	Never observed	Never observed	Never observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Customer Service	SIM card related	Found guilty(Sued penalized)
Case16	Rarely observed	Very rarely observed	Very rarely observed	Frequently observed	Occasionally observed	Occasionally observed	Occasionally observed	Occasionally observed	Never observed	Occasionally observed	Very rarely observed	Rarely observed	Very rarely observed	Frequently observed	Very rarely observed	Frequently observed	Rarely observed	Rarely observed	Frequently observed	Very rarely observed	Information Security	VAS related fraud	Found guilty(Sued penalized)
Case17	Very rarely observed	Occasionally observed	Occasionally observed	Very rarely observed	Verified identity served	Very rarely observed	Never observed	Occasionally observed	Very rarely observed	Very rarely observed	Verified identity served	Occasionally observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Frequently observed	Verified identity served	Occasionally observed	Verified identity served	Information Security	False certification	Found guilty(Sued penalized)
Case18	Never observed	Never observed	Rarely observed	Very rarely observed	Frequently observed	Never observed	Occasionally observed	Very rarely observed	Never observed	Rarely observed	Occasionally observed	Never observed	Very rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Never observed	Verified identity served	Very rarely observed	Occasionally observed	Sales	False certification	Found guilty(Sued penalized)
Case19	Never observed	Never observed	Rarely observed	Very rarely observed	Occasionally observed	Never observed	Rarely observed	Never observed	Never observed	Very rarely observed	Rarely observed	Never observed	Very rarely observed	Very rarely observed	Never observed	Very rarely observed	Never observed	Very rarely observed	Very rarely observed	Very rarely observed	Information Security	Benefit related	Found guilty(Sued penalized)
Case20	Rarely observed	Occasionally observed	Occasionally observed	Very rarely observed	Rarely observed	Very rarely observed	Rarely observed	Very rarely observed	Rarely observed	Very rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Occasionally observed	Very rarely observed	Occasionally observed	Rarely observed	Rarely observed	Information Security	Benefit related	Found guilty(Sued penalized)
Case21	Occasionally observed	Occasionally observed	Occasionally observed	Rarely observed	Rarely observed	Very rarely observed	Rarely observed	Very rarely observed	Rarely observed	Rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Occasionally observed	Never observed	Occasionally observed	Rarely observed	Very rarely observed	Customer Service	Data theft related fraud	Found guilty(Sued penalized)
Case22	Never observed	Very rarely observed	Rarely observed	Rarely observed	Very rarely observed	Very rarely observed	Never observed	Occasionally observed	Never observed	Very rarely observed	Very rarely observed	Rarely observed	Very rarely observed	Rarely observed	Never observed	Very rarely observed	Very rarely observed	Rarely observed	Rarely observed	Never observed	Sales	SIM card related	Found guilty(Sued penalized)

Database: insider, Table: insider, Purpose: Dumping data

CaseID	Self_Centeredness	Absenteeism	Disengagement	Lack_of_Dependability	Addictions	Disgruntlement	Stress	Deception	Not_Accepting_Feedback	Personal_Issues	Peer_Pressure	Belonging	Anger_Management_Issues	Inattentiveness	Disregard_for_Authority	Contradictional_Behavior	Outside_working_hours	Performance	Unexplained_absenteeism_of_weekdays	Carelessness	Department	Fraud_Type	Taken_Action
	served	systems	served	served	systems	systems	served	abysbserved	served	systems	served	served	systems	served	served	systems	systems	served	served	served	empathy	Absence	Office Issue
Case12	veryrare systems	veryrare systems	veryrare systems	Rarelyobserved	Rarelyobserved	Veryrare systems	Rarelyobserved	Neverobserved	Neverobserved	veryrare systems	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Neverobserved	Occasionallyobserved	Rarelyobserved	Veryrare systems	Rarelyobserved	Occasionallyobserved	Customer Service	Data Theft, Identity Theft	Fraud & Office Issue
Case24	Frequently systems	Frequently systems	Rarelyobserved	Frequently systems	Frequently systems	Veryrare systems	Occasionallyobserved	Occasionallyobserved	Occasionallyobserved	Frequently systems	Occasionallyobserved	Rarelyobserved	Occasionallyobserved	Occasionallyobserved	Rarelyobserved	Occasionallyobserved	Frequently systems	Occasionallyobserved	Occasionallyobserved	Rarelyobserved	Management	Insurance Fraud	Fraud & Office Issue
Case25	Veryrare systems	Neverobserved	Rarelyobserved	Occasionallyobserved	Veryrare systems	Neverobserved	Veryrare systems	Occasionallyobserved	Rarelyobserved	Veryrare systems	Frequently systems	Veryrare systems	Rarelyobserved	Neverobserved	Occasionallyobserved	Occasionallyobserved	Veryrare systems	Veryrare systems	Veryrare systems	Neverobserved	Customer Service	Data Theft, Identity Theft	Fraud & Office Issue
Case29	Occasionallyobserved	Frequently systems	Occasionallyobserved	Frequently systems	Neverobserved	Neverobserved	Frequently systems	Occasionallyobserved	Occasionallyobserved	Frequently systems	Occasionallyobserved	Rarelyobserved	Frequently systems	Frequently systems	Rarelyobserved	Veryrare systems	Frequently systems	Veryrare systems	Frequently systems	Veryrare systems	Customer Service	Online Identity Theft	Fraud & Office Issue
Case37	Frequently systems	Neverobserved	Rarelyobserved	Rarelyobserved	Veryrare systems	Occasionallyobserved	Frequently systems	Veryrare systems	Veryrare systems	Frequently systems	Veryrare systems	Neverobserved	Rarelyobserved	Occasionallyobserved	Veryrare systems	Frequently systems	Veryrare systems	Rarelyobserved	Neverobserved	Neverobserved	Management	Data Theft, Identity Theft	Fraud & Office Issue
Case39	Neverobserved	Neverobserved	Veryrare systems	Neverobserved	Veryrare systems	Neverobserved	Occasionallyobserved	Neverobserved	Neverobserved	Veryrare systems	Rarelyobserved	Neverobserved	Veryrare systems	Veryrare systems	Neverobserved	Frequently systems	Veryrare systems	Neverobserved	Frequently systems	Frequently systems	Healthcare Facilities	Insurance Fraud	Fraud & Office Issue
Case75	Rarelyobserved	Veryfrequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Neverobserved	Veryfrequently systems	Veryfrequently systems	Occasionallyobserved	Frequently systems	Frequently systems	Frequently systems	Veryfrequently systems	Frequently systems	Rarelyobserved	Veryfrequently systems	Frequently systems	Veryfrequently systems	Veryrare systems	Veryrare systems	Sales	Data Theft, Identity Theft	Fraud & Office Issue
Case91	Veryfrequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Neverobserved	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Neverobserved	Customer Service	Gift card related	Fraud & Office Issue
Case101	Frequently systems	Occasionallyobserved	Rarelyobserved	Neverobserved	Veryfrequently systems	Neverobserved	Occasionallyobserved	Occasionallyobserved	Occasionallyobserved	Veryfrequently systems	Frequently systems	Rarelyobserved	Occasionallyobserved	Occasionallyobserved	Occasionallyobserved	Veryfrequently systems	Occasionallyobserved	Frequently systems	Veryfrequently systems	Frequently systems	Management	Data Theft, Identity Theft	Fraud & Office Issue
Case102	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryrare systems	Veryfrequently systems	Veryfrequently systems	Rarelyobserved	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Occasionallyobserved	Veryfrequently systems	Frequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Information Security	SIM related Fraud	Fraud & Office Issue
Case103	Occasionallyobserved	Occasionallyobserved	Veryrare systems	Frequently systems	Veryfrequently systems	Occasionallyobserved	Frequently systems	Frequently systems	Veryrare systems	Veryrare systems	Rarelyobserved	Veryrare systems	Frequently systems	Occasionallyobserved	Rarelyobserved	Frequently systems	Rarelyobserved	Veryrare systems	Veryrare systems	Veryrare systems	Customer Service	SIM related Fraud	Fraud & Office Issue
Case104	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Veryrare systems	Information Security	Identity Theft	Fraud & Office Issue
Case105	Frequently systems	Frequently systems	Occasionallyobserved	Frequently systems	Frequently systems	Veryrare systems	Frequently systems	Veryfrequently systems	Rarelyobserved	Frequently systems	Veryfrequently systems	Frequently systems	Occasionallyobserved	Frequently systems	Rarelyobserved	Frequently systems	Frequently systems	Occasionallyobserved	Frequently systems	Rarelyobserved	Information Security	False ref Whistleblower	Fraud & Office Issue
Case106	Occasionallyobserved	Occasionallyobserved	Occasionallyobserved	Occasionallyobserved	Frequently systems	Rarelyobserved	Veryfrequently systems	Veryfrequently systems	Veryrare systems	Veryrare systems	Veryfrequently systems	Occasionallyobserved	Rarelyobserved	Veryfrequently systems	Rarelyobserved	Veryfrequently systems	Occasionallyobserved	Frequently systems	Occasionallyobserved	Frequently systems	Healthcare Facilities	Insurance Fraud	Fraud & Office Issue
Case107	Rarelyobserved	Veryrare systems	Veryrare systems	Rarelyobserved	Frequently systems	Occasionallyobserved	Frequently systems	Occasionallyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Occasionallyobserved	Rarelyobserved	Occasionallyobserved	Veryrare systems	Frequently systems	Veryrare systems	Occasionallyobserved	Veryrare systems	Sales	Insurance Fraud	Fraud & Office Issue
Case108	Frequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Neverobserved	Veryfrequently systems	Frequently systems	Veryfrequently systems	Frequently systems	Frequently systems	Occasionallyobserved	Rarelyobserved	Occasionallyobserved	Rarelyobserved	Veryfrequently systems	Occasionallyobserved	Rarelyobserved	Veryfrequently systems	Neverobserved	Customer Service	Data Theft, Identity Theft	Fraud & Office Issue
Case109	Frequently systems	Rarelyobserved	Occasionallyobserved	Veryfrequently systems	Frequently systems	Rarelyobserved	Veryfrequently systems	Veryfrequently systems	Rarelyobserved	Veryfrequently systems	Veryfrequently systems	Rarelyobserved	Frequently systems	Frequently systems	Veryfrequently systems	Veryfrequently systems	Veryfrequently systems	Rarelyobserved	Occasionallyobserved	Veryfrequently systems	Management	Data Theft, Identity Theft	Fraud & Office Issue
Case82	Neverobserved	Veryrare systems	Veryrare systems	Veryrare systems	Rarelyobserved	Neverobserved	Rarelyobserved	Veryrare systems	Neverobserved	Neverobserved	Neverobserved	Veryrare systems	Veryrare systems	Veryrare systems	Neverobserved	Veryrare systems	Veryrare systems	Neverobserved	Veryrare systems	Veryrare systems	Sales	SIM related Fraud	Fraud & Office Issue
Case42	Rarelyobserved	Neverobserved	Rarelyobserved	Rarelyobserved	Veryfrequently systems	Neverobserved	Rarelyobserved	Rarelyobserved	Veryrare systems	Rarelyobserved	Frequently systems	Veryrare systems	Veryrare systems	Neverobserved	Veryrare systems	Occasionallyobserved	Frequently systems	Veryrare systems	Veryrare systems	Veryrare systems	Finance	Insurance Fraud	Fraud & Office Issue
Case42	Frequently systems	Frequently systems	Frequently systems	Frequently systems	Rarelyobserved	Veryfrequently systems	Frequently systems	Veryrare systems	Frequently systems	Frequently systems	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Rarelyobserved	Finance	Insurance Fraud	Fraud & Office Issue

Database: insider, Table: insider, Purpose: Dumping data



Database: Insider, Table: Insider, Purpose: Dumping data

CaseID	Self_Centeredness	Absenteeism	Disengagement	Lack_of_Dependability	Addictions	Disgruntlement	Stress	Deception	Not_Accepting_Feedback	Personal_Issues	Peer_Pressure	[illegible]	Anger_Management_Issues	[illegible]	Disregard_for_Authority	Confrontational_Behavior	Outside_working_hours	Performance	[illegible]	[illegible]	Department	Fraud_Type	Taken_Action
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Appendix IV Discipline measure taken on fraudulent employees at Ethio telecom

n°66

ከ2009 ግማሽ በጀት ዓመት ጀምሮ የተወሰዱ አስተዳደራዊ የዲሲፒሊን እርምጃዎች

ኢትዮ ቴሌኮም ከ2009 ግማሽ በጀት ዓመት ጀምሮ በኩባንያው ውስጥ የተለያዩ የዲሲፕሊን ጥፋት የፈጸሙ ሠራተኞች ላይ ተገቢውን የማጣራት ሥራ በማከናወን ተመጣጣኝ አስተዳደራዊ የቅጣት እርምጃ የወሰደ ሲሆን ለአስተማሪነቱ ሞና ሞናዎቹ እንደሚከተለው ቀርበዋል።

የሥራ ክፍል	የጥፋቱ ዓይነት	የተወሰደ እርምጃ
ደቡብ ምስራብ ሪጂን	ከሀዋቃቅንና አነስተኛ ኢንተርፕራይዝ ማህበራት ጋር በተደረገ የውል ስምምነት ኩባንያው ካስቀመጠው የተናጠል ዋጋ በላይ ጨምሮ በመፈራረም ጉዳት ማድረስና የተሰጠን የሥራ ድርሻ ችላ በማለት ሥራን በአግባቡ አለማከናወን	የ21.45 ቀን ደመወዝ ቅጣት
ደቡብ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ የገንዘብ ማጭበርበር	ከሥራ ደረጃ ዝቅ ማድረግ
ደቡብ ሪጂን	የግል ጥቅም ለማግኘት ሲባል የኩባንያውን ደንብና መመሪያ በመጣስ የተጭበረበረ /ሐሰተኛ/ የትምህርት ማስረጃ ማቅረብ	ከሥራ ማሰናበት
ማዕከላዊ አዲስ አበባ ዞን ቁና መ/ቤት ሶርሲንግ ሳቪዝን	የግል ጥቅም ለማግኘት ሲባል የኩባንያውን ደንብና መመሪያ በመጣስ የመ/ቤቱን ተሽከርካሪ ንጣ መሸጥ	ከሥራ ማሰናበት

ሰሜን አዲስ አበባ ዞን	የኩባንያውን ደንብና መመሪያ በመጣስ ለሌላ ተቋም በቋሚነት ተቀጥረው በመስራት	ከሥራ ማሰናበት
የደንበኞች አገልግሎት ዲቪዥን	የኩባንያውን ደንብና መመሪያ በመጣስ ሐሰተኛ/የተጭበረበረ የህክምና/የሕመም ፈቃድ ማስረጃ ማቅረብ እናም ክዶ መከራከር	ከሥራ ማሰናበት
ደቡብ ሪጂን	የግል ጥቅም ለማግኘት ሲባል የኩባንያውን ደንብና መመሪያ በመጣስ የተጭበረበረ /ሐሰተኛ/ የትምህርት ማስረጃ ማቅረብ	ከሥራ ማሰናበት
ሪዚደንሻል ሲልስ ሪዚደንሻል ሲልስ ኢንተርፕራይዝ ሲልስ	የግል ጥቅም ለማግኘት ሲባል የኩባንያውን ደንብና መመሪያ በመጣስ 10 [illegible] ቁጥሮችን መያዝና አለአግባብ ለሦስተኛ ወገን አሳልፎ መሸጥ	የ15 ቀን ደመወዝ ቅጣት
ኔትወርክ ዲቪዥን	የኩባንያውን ደንብና መመሪያ በመጣስ ለሌላ ተቋም በቋሚነት ተቀጥረው በመስራት	ከሥራ ማሰናበት
ምስራቅ አዲስ አበባ ዞን ምስራቅ አዲስ አበባ ዞን	የግል ጥቅም ለማግኘት ሲባል የኩባንያውን ደንብና መመሪያ በመጣስ የመ/ቤቱን ንብረት ለግል ጥቅም በማዋል	የ15 ቀን ደመወዝ ቅጣት
ሰሜን አዲስ አበባ ዞን	የኩባንያውን ደንብና መመሪያ በመጣስ በሥራ ቦታ ላይ ፀብ በመጫርና አምባጓሮ በመፍጠር	የ15 ቀን ደመወዝ ቅጣት
ደቡብ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ ሐሰተኛ/የተጭበረበረ የህክምና/የሕመም ፈቃድ ማስረጃ በማቅረብና የኩባንያውን ገንዘብ ለግል ጥቅም ማዋል	ከሥራ ማሰናበት

ኔትወርክ ዲቪዥን	የግል ጥቅም ለማግኘት ቢባል የኩባንያውን ደንብና መመሪያ በመጣስ የተሞከረበረ /ሐሰተኛ/ የትምህርት ማስረጃ ማቅረብ	ከሥራ ማሰናበት
ደቡብ ምዕራብ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ የሰርቪስ ቁጥሮች ሙስ በሙስ የነበሰት በንደ፣ የተሳሳተ ስም እና ሀሰተኛ ሌሎች መረጃዎች አስገብቱው ሽያጭ ማከናወን	የ15 ቀን ደመወዝ ቅጣት
ምስራቅ አዲስ አበባ ዞን	የኩባንያውን ደንብና መመሪያ በመጣስ በተደጋጋሚ ያለፈቃድ ከሥራ ገበታ መቅረት፣ የእለት ሽያጭ በወቅቱ ገቢ አለማደረግ	የ15 ቀን ደመወዝ ቅጣት
ደቡብ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ በተደጋጋሚ ያለፈቃድ ከሥራ ገበታ መቅረት፣ የእለት ሽያጭ ለግል ጥቅም ማዋል	ከሥራ ማሰናበት
የደንበኞች አገልግሎት ዲቪዥን	የግል ጥቅም ለማግኘት ቢባል የኩባንያውን ደንብና መመሪያ በመጣስ የተሞከረበረ /ሐሰተኛ/ የትምህርት ማስረጃ ማቅረብ	ከሥራ ማሰናበት
ጋምቤላ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ የቀን ሠራተኛ ፈርማ አስመስለው በመፈረም ገንዘቡን ለግል ጥቅም ማዋል	የ15 ቀን ደመወዝ ቅጣት
ምስራቅ አዲስ አበባ ዞን	የኩባንያውን ደንብና መመሪያ በመጣስ ከኩባንያው አውቅና ውጪ መሰመር ማዘመር	የ15 ቀን ደመወዝ ቅጣት
ምስራቅ አዲስ አበባ ዞን		
ምዕራብ ሪጂን	የኩባንያውን ደንብና መመሪያ በመጣስ የሽያጭ ማስከሉን ገንዘብ ማጉደል	ከሥራ ማሰናበት

የሰው ኃይል ዲቪዥን
ሚያዝያ 2010 ዓ.ም

በ2011 ዓ.ም የተወሰዱ የዲሲፕሊን እርምጃዎችን ስለማሳወቅ

ኢትዮ ቴሌኮም በ2011 በጀት ዓመት በኩባንያው የተለያዩ የስራ ክፍሎችና ሪጂኖች የዲሲፕሊን ጥፋት የፈጸሙ ሠራተኞች ላይ በኩባንያው ህብረት ስምምነትና በዲሲፕሊን ኮሚቴው አሰራር መሰረት ተገቢውን የማጣራት ሥራ በማከናወን እንደጥፋታቸው ደረጃ ከአስራ አምስት ቀን የደመወዝ ቅጣት እንሰቶ እስከ ስራ ስንብት የሚደርስ አስተዳደራዊ የቅጣት እርምጃ የወሰደ ሲሆን ለአስተማሪነቱ ዋና ዋናዎቹ እንደሚከተለው ቀርበዋል።

ከሰንድ ማጭበርበር ጋር በተያያዘ

- ደቡብ ምዕራብ ምዕራብ ሪጂን /በጋምቤላ/ የቀን ሰራተኛ ፊርማ አስመስሎ በመፈረምና ከፍያ በመቀበል ለግል ጥቅሙ ያዋለ አንድ ሰራተኛ ከስራ ተሰናብቷል።
- በሰሜን ምዕራብ ሪጂን ሃሰተኛ የሂሳብ ሰንድ በማዘጋጀትና አስመስሎ በመፈረም የማጭበርበር ድርጊት ጥፋተኛ ሆኖ የተገኘ አንድ ሰራተኛ ከስራ ተሰናብቷል።
- በደቡብ ደቡብ ምዕራብ ሪጂን/ወላይታ/ ከቀን ሰራተኞች ከፍያ ጋር በተያያዘ የተጭበረበረ የከፍያ ሰንድ በአግባቡ ሳያጣራ ከፍያው እንዲፈጸም ያሳለፉ ሶስት ሰራተኞች የጽሁፍ ማስጠንቀቂያ እና የአስራ አምስት ቀን ደመወዝ ቅጣት ተወሰኖባቸዋል።
- በደቡብ ደቡብ ምዕራብ ሪጂን/ወላይታ/ የተጭበረበረ የከፍያ ሰንድ በማዘጋጀትና የቀን ሰራተኞችን ፊርማ አመሳስሎ በመፈረም ለግል ጥቅሙ ያዋለ አንድ ሰራተኛ ከስራ ተሰናብቷል።
- የህክምና የእረፍት ወረቀትን በመያዝ የተጭበረበረ የህክምና ፈቃድ ያቀረበ አንድ የጥሪ ማስከል ሰራተኛ ከደረጃ ዝቅ በማድረግ እንዲቀጣ ተወስኗል።

ከማጭበርበር /ፍራውድ/ ጋር በተያያዘ

- የተቋሙን የሽያጭ መመሪያ በመተላለፍ የቫኒቲ ሰርቪስ ቁጥሮችን ትክክለኛ ባልሆነ መንገድ በመሸጥና ነጻ ፓኒጆችን ለግል ጥቅማቸው ያለአግባብ በመጠቀም ጥፋተኛ ሆነው የተገኙ ሁለት የደቡብ ምዕራብ ሪጂን ሠራተኞች እና አንድ የሰሜን ምዕራብ ሪጂን ሠራተኛ ከስራ እንዲሰናበቱ ተወስኗል።

ከሌሎች ጥፋቶች ጋር በተያያዘ

- በተቋሙ ተሽከርካሪ የተለያየ ዓይነት የኮንትሮባንድ እቃ ሞኖ ሲገዝ የተያዘ አንድ የምሰራቅ ሪጂን ሠራተኛ ከሰራ እንዲሰናበት ተወስኗል።
- የሰራ ሰምሪት ሳይሰጠው የተቋሙን ተሽከርካሪ ለአንድ ቀን ይዞ የተሰወረ የፍሊትና ፋሲሊቲ ዲቪዥን ሠራተኛ የጽሁፍ ማስጠንቀቂያ እና የአሰራ አምስት ቀን ደመወዝ ቅጣት ተወስኖበታል።
- ለጥገና ጋራዥ የገባን ተሽከርካሪ ከተቋሙ እውቅና ውጭ ከጋራዥ በማውጣትና ለአራት ቀን ይዞ በመጥፋት ጥፋተኛ ሆኖ የተገኘ አንድ የፍሊትና ፋሲሊቲ ዲቪዥን ሰራተኛ ከደረጃ ዝቅ በማድረግ እንዲቀጣ ተወስኗል።
- በኮባንያው መደበኛ የሰራ ሰዓት የዓመት ፈቃድ ሳይሞላ ትምህርት ሲማር የተገኘ ምሰራብ ምሰራብ ሪጂን /የአሶሳ/ ሰራተኛ የጽሁፍ ማስጠንቀቂያ እና የአሰራ አምስት ቀን ደመወዝ ቅጣት ተወስኖበታል።

በኢትዮ ቴሌኮም ሁሉም ሰራተኛ በታማኝነት፣ በቅንነት፣ በተቆርቋሪነትና በውጤታማነት ሰራውን በማከናወን እራሱንም ሆነ ኩባንያውን ወደሚቀጥለው የለውጥና የእድገት ደረጃ ለማሻገር ጥረት ማድረግ በሚጠበቅበት በአሁኑ ወቅት የተቋሙን እሴትና የመልካም ሰራተኞች ሰም በሚጎዳ መልክ ፍፁም ተቀባይነት የሌለው የዲሲፕሊን ግድፈት እየተፈፀመ መሆኑ ታውቋል። በተለይ ኩባንያውን በማሜበርበር የግል ጥቅም ለማግኘትም ሆነ ለሶስተኛ ወገን ጥቅም ለማስገኘት የሚደረግ ድርጊት ፈፅሞ ተቀባይነት የሌለውና ኩባንያው የማይታገሰው ጥፋትም ወንጀልም መሆኑን መገንዘብ ያስፈልጋል። በአሁኑ ወቅትም ሌሎች ተመሳሳይና ተቀራራቢ የዲሲፕሊን ግድፈቶች በመጣራት ላይ ሲሆኑ ውጤቱ እንደተጠናቀቀ ለሰራተኞች የምናሳውቅ መሆኑን እንገልፃለን።

በመሆኑም በቀጣይም በማንኛውም የተቋሙን አሰራር በሚጥስ የዲሲፕሊን ግድፈት ተነፋለው በሚገኙ ሠራተኞች ላይ ተቋሙ የሚወስደውን እርምጃ አጠናክሮ እንደሚቀጥልና እንደአስፈላጊነቱም በህግ አግባብ እንዲጠየቁ እንደሚያደርግ እንዲሁም በየወቅቱ ውሳኔዎቹን የምናሳውቅ መሆኑን እየገለጽን ሁሉም ሠራተኛ የተቋሙን ህግና ደንብ በማክበርና ሌሎችንም በማስተማር፤ የዲሲፕሊን ግድፈቶች ሲፈጸሙም በማጋለጥ የበኩሉን ድርሻ እንዲወጣ እናሰገንዝባለን።

የሰሙ ኃይል ዲቪዥን
መጋቢት 2011 ዓ.ም

Published by: Internal Communications Section

Appendix V Letter of Support

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ትምህርት ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Ethio telecom

Date: December 26, 2018
Ref: SIS/22/2018/11

To whom it may Concern

Dear Sir/Madam,

Student Yohanes Halefom (ID No GSE/5697/09) is a graduae student at the School of Information Science, Addis Ababa University. She is currently conducting a MSc Thesis research under the title "Case baded reasoning for insider threat behavior identification and control".

I would like to thank you in advanced for all the assistance that you would provide to the student.

With Regards,

Tibebe Beshah (PhD)
Head, School of Information Science

IT & Network Security

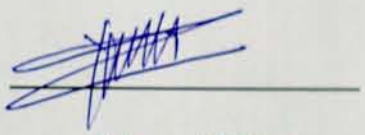
22-01-2019

+251-(11)-122-91-91

1176

Declaration

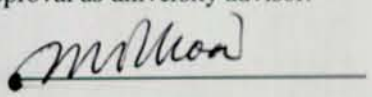
I declare that the thesis is my original work and has not been presented for a degree in any other university.



Yohanes Halefom

June 2019

This thesis has been submitted for examination with my approval as university advisor.



Million Meshesha (PhD)