



Weaknesses and Security Threats: Emerging Enterprises

Ahmed Dheyaa Basha

Faculty of Computer Science & Information Technology

University of Sumer

Thi-Qar- ALQul, aa 64003

Iraq

Abstract: Different obstacles in managing Emerging Enterprises (EEs), in term of weaknesses and security threats are investigated. Conceptual framework detailed with possessions and threat ranking is suggested. The framework objectives refer to support EEs to prohibit and alleviate threats and weakness in possessions successfully. The model of framework security issues included of weaknesses, possessor, threats, proxies of threat, precautionary measures, hazards and possessions, as well as their relationship; while possessions ranking is an approach based on value, and threat ranking is depends on timeline of attack.

Keywords: Weaknesses, Security Threats, Emerging Enterprises (EEs).

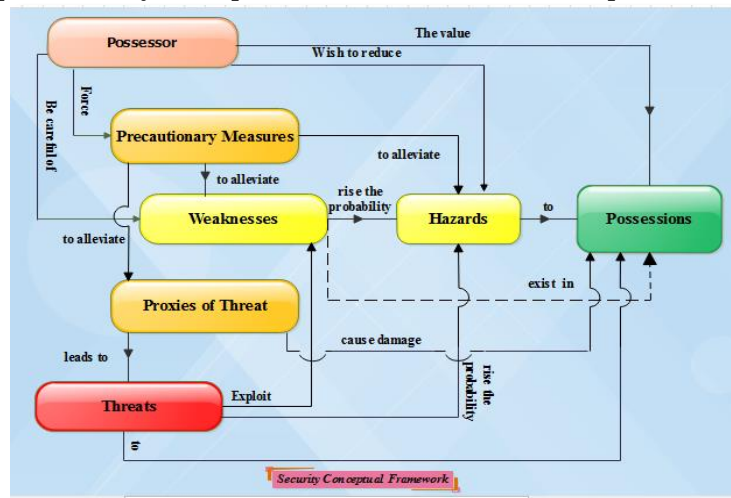
I. Introduction

Managing different security threats and weaknesses in possessions are two major fundamental challenges for EEs, Whitman et al. [3, 15]. Weaknesses in possessions are vulnerabilities in possessions in case of Lacking of security procedures, physical or technical controls that could be invested or exploited or liable possessions to harm, Hsiao et al. [10]. In this respect, harm to possession happen in the form obstruction, interruption, demolition, detection, amendment of data to denial or deportation of service. For instance in last decade the code red episode exploited a buffer surplus in library module from Microsoft Windows' Internet Information Servers [9]. This episode allowed it to damageand infects thousands of computers, and lost millions of dollars. In addition the worms also exploited known weaknesses in computer system, Rittinghouse et al. [21]. These multi threats affect directly on pillars of security include integrity, reliability, availability and confidentiality of computer network services. Moreover, consideration of security threats also used as attack by proxies of threat in denial of service (DoS) and distributed of service (DDoS) attacks (for example computer worms, Basha et al. [8]. These threats affect on pillars of security include (integrity, reliability, availability and confidentiality of computer network services), Chen et al. [4]. The financial losses are very significant in terms of the impact of threats on different organizations according to many reports via annual computer crimes and various security surveys, the estimated financial losses about computer security crimes and incidents were millions of dollars [21]. The four major categories of threats considered roughly more than 70% of total losses were in: (i) theft of special proprietary information, (ii) viruses, (iii) unauthorized access by users, and (iv) mobile and laptop hardware theft. According to CSI/FBI crimes survey, different types of malicious codes such (viruses) have been number-one, and these threats dominant for several years [13]. Since that weaknesses in possessions and the threats that utilize them cannot be fully avoided [5]. It is urgent that both must be appropriately alleviated. In spite of existing different defense models cannot debacle all threats [14]. This is because majority of models lacking of detailed representation of the dynamics of threats extension in many types of networks, hardly focusing on separated techniques to alleviate threats, Yang et al. [6], [18]. Comprehension all weaknesses is critical issue to realize the threats they represent. Rapidly managing weaknesses and threats requires both a detailed comprehension of concepts and diverse relationships, Tipton et al. [12]. Like an understanding can support EEs in achievement the correct mix of protection controls to identify and alleviate both threats and weaknesses. Essential to this are models that in abundance represent different relationships and security concepts in terms of possessor, weaknesses, threats, and proxies of threats, precautionary measures, hazards and possessions. The advantages of this processing to EEs are that it allows them: a) correctly classify valued possessions, b) neatly identify weaknesses in classified valued possessions, c) alleviate and identify possibility threats imposed on possessions, d) fitly evaluate linked hazards, e) appropriately classify threats and their proxies of threat; and thence provide convenient and precautionary measures effective to reduce hazards to valued possessions in return, Vanhoucke et al. [19]. Consequently, contribution in this article is therefore, to achieve a processing to effective security management via a conceptual framework that support organizations to classify possessions, alleviate threats and identify both weaknesses and threats. In this paper Models that evaluate both weaknesses and threats together provide precautionary measures that are closely related more effective, convenient and timely. While second section discusses definition of terms and related work; third section tests the security conceptual framework in managing threats and weaknesses in possessions. In addition, forth section this article investigate security threats in terms of their impacts, ranking and deployment dynamics based on attack timeline; moreover summarize with a brief of conclusion in fifth section.

II. Related Work

Research into weaknesses and threats of sciences computer systems increased because it's evolving track and considerable economic impact on all organizations, Khalfan et al. [2, 16].

Figure 1: Explain Security Conceptual Framework for seven concepts and their relationships.



The General Standards (GS):- predominantly ISO/IEC 15408 comprise one from a few models that address weaknesses and threats with each other, illustrate representation and variety relationships of security concepts including possessor, protection, hazards and possessions. But GS's model is restricted in perspective due to it neither comprise weaknesses in possessions in its representation nor variety relationships of weaknesses to other security concepts, Jamaludin et al. [8,15]. Ordinarily the GS's model is beneficial for evaluation of various engineering products and subsequently necessary in its own rights, in this case the model needs to develop to comprise other security concepts necessary in protecting possessions, because ever-increasing accidents of weaknesses in possessions. A model of threat ranking and precautionary measures was proposed by, Susanto et al. [15]. Which target to identify possible results to an attack? In addition, the model focuses on attacks and output of outcomes, thus relationships of security causes such as weaknesses in possessions were not obviously covered. Despite, contributions in the literature, but still or most of them either specifically addressing weaknesses assessment according to, Heagney et al. [18], or about threats, Graham et al. [10,7]. Therefore, Security Conceptual framework in this article includes both threats and a weaknesses issue, Moreover relationships of security concepts considers prominently a step forward as explained in Fig.1.

A. Description and Definition

Generally computer security is set of procedures to protection computer networks that achieve main objectives including, integrity, confidentiality, and availability of information system resources, which comprise software, hardware, data or information, firmware, and telecommunications explained by Vanhoucke [20]. Subsequently the key objectives of weaknesses and managing threats in system are to support and protect all computer networks in addition to their communications in order to maintain the: (a) Integrity of all computer networks, moreover data and information. In which a requirement aimed to verification that all computer networks and their services provided are precise, integral, symmetrical, original and timely. (b) Confidentiality of communications and systems. In which a requirement to remove unauthorized disclosure of communications and systems either purposely or inadvertently omitted, Almunawar et al. [13]. (c) Availability of services provided and computer networks. In which a requirement to purpose ensure systems and their services provided are available at accepted different levels to legal entities [16]. Majority of threats to all computer networks usually defined as multi events, different circumstances or entities with ability to create inflict damage or deform ordinary security operations via exploiting weaknesses in systems, Ruuska et al. [17]. While the damage is defined as the perversion or breach of the, integrity, confidentiality and availability of all computer network, through different forms of modification, demolition, detection, obstruction of data or denial of multi services. The possessions are defined as a base value and importance to the possessor, which comprise data, information, network, programs and communication infrastructures, Rittinghouse et al. [21].

III. How Managing Security Threats and Weaknesses in Possessions for Design Framework

The accomplished conceptual framework security is adapted from general Standards for ISO/IEC 15408 [3], this article explain seven concepts for security and their relationships explained in Figure 1, as follows: a) possessions' Possessor b) weaknesses in possessions c) proxies of threat d) Threats and how exploit weaknesses in possessions e) hazards that outcome due to threats and weaknesses f) Precautionary measures imposed to avoid and alleviate threats, weaknesses and hazards, and finally g) Valued Possessions of the EEs. Thus, the main aim of security conceptual framework as stated in Fig.1. is to support different organizations to realize what is required to protect the possessions, and what should be available to protected from (weaknesses, threats, and linked hazards) and protected (precautionary measures). Firstly, the framework supports EEs to understand important possessions to them, specify what should be prepared to protected and vulnerabilities that exist in those possessions. Secondly, to evaluate what can attain these vulnerabilities, and eventually, to determine on what can be essential to block and alleviate identified threats and weaknesses, are explained in Table 1.

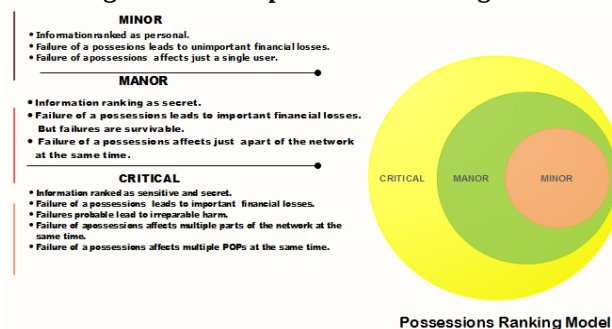
Table1: Characterization of the security conceptual framework

Concepts Security	Characterization
Possessors	Organizations or persons who own the possessions.in which Possessors value their possessions, in addition they realize of the weaknesses relate to their possessions, but they in the end want to minimize the probability of their possessions from threats , so require precautionary measures to prohibit or alleviate weaknesses, threats and linked hazards to possessions.
Precautionary measures	Include security controls (protections) imposed by the possessions possessors to alleviate weaknesses in possessions, threats to possessions and hazard to possessions.
weaknesses	Include shortcomings in possessions or protection controls that could lead to breach in security when used by threats that boost the Probability of hazards to possessions.
Proxies of threat	Comprise multi entities with the ability to introduce threats to possessions.
Threats	Comprise multi entities that used weaknesses in possessions, thereafter boosting probability of hazards to damage or cause damage to assets.
Hazards	The likelihood (probability) that possessions may be exposed by threats.
Possessions	Systems, all information, data, different applications and programs owned by the possessors.

A. Possessions Ranking

Possessions ranking schemas are utilized by organizations to locate which possessions such as (information, applications, program, data, and system infrastructure) are decisive in their processing. In this article developed a possessions ranking to help organizations in doing this, see Fig.2. In this respect developed ranking is flexible, simple and adaptive. As a 'rough processing guideline', in addition the ranking is simple, robust and completely modest to implement, on the contrary to ranking that presuppose strict implementation time and numerous explanations or different interpretations, Chen et al. [4]. Moreover, majority of schemas are difficult to recognize in terms of classify and time, therefore in practically useless in process environment. The oppressions ranking model and its classifications are flexible and can be modified via an organization to either include or exclude conveniently other domains. For instance, numerous organizations may comprise such fields as "unimportant" for possessions not ranked as major, minor or critical, according to "The Rainbow Books" information possessions can be classified as, 'sensitive', 'secret' and 'top secret', Susanto et al. [15]. In this case, the ranking included 3- grades ranking as unimportant major, minor, and critical. With "unimportant" possessions, the failure of a possessions leads to unimportant financial losses, consequently failures are just potential, for instance, admonition threats or informational, for instance system warnings or fault in a computer program (System warnings). In similar manner, ranking model is adaptive due to it is not merely designed to be used in computing; but it is readily adaptable to multi business operations.

Figure 2: Shows possessions ranking model



B. Identify Security Weaknesses and Evaluation

Weaknesses and Evaluation is a reconsidering of security situation of operational systems for aim of distinguishes potential weaknesses in possessions, Liu et al. [11].When weaknesses which have been identified; convenient

alleviation controls are implemented to save valued possessions [12]. Since weaknesses evaluation are not exclusively led to identify potential weaknesses, but also to achieve lost precautionary measures, Basha et al. [7]. It is therefore urgent that periodic weaknesses evaluation is completed to save critical possessions. The advantages of security weaknesses evaluation comprise:

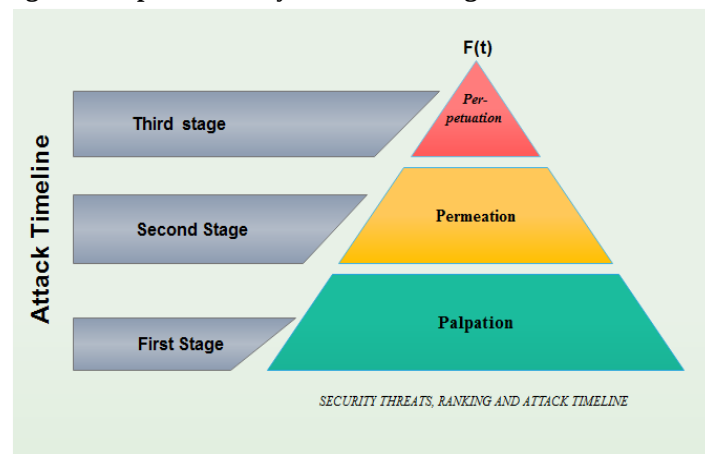
- Determine an organization's possessions (data, programs, information, infrastructures, systems and network, applications).
- Classify possessions specified based on their importance to the organization, like "critical" or "non-critical". In this respect, the ranking according to the distributed methodology.
- 3.Determine critical possessions to an organization for instance, information, like (marketing "ranked" types of military information).Moreover identify and determine different infrastructure such as network, systems, stores, processes as well as transmits various organization's critical information.
- Identify the security situation of possessions to determine potential weaknesses in them.
- Identify linked security hazards on possessions include information, software, content and infrastructure and comprise: types of end user devices like (PDAs and PCs), moreover user support devices as well as actual content and furthermore.
- Identify different security requirements and coordination the correct mix of precautionary measures.
- Link missing control, save measures and take into account requirements which carried out incorrectly or not implemented, to purpose of saving critical possessions. And eventually, to recommend saving control (precautionary measures) to alleviate identified weaknesses.

IV. Security Threats, Ranking and Attack Timeline

A. Threats and Attack Timeline

To test how security threats exploit weaknesses in possessions, a requirement is to achieve ranking of threats.in different studies, threats have been ranked depended on weaknesses, according to Williams et al. [9]. Their study concentrated on identifying potential weaknesses, and how an attacker may exploits to damage possessions to provide convenient precautionary measures. Therefore, this study provide effective and timely precautionary measures a ranking of security threats depended on propagation timeline is to test when in a threatpenetration cause most serious damage to possessions , and what precautionary measures are possible during all specific stage to effectively and timely alleviate the threat, Susanto et al. [16]. Consequently, ranking of security threats depended on attack timeline is recognized clearly. In this respect, the developed security threats ranking is a three stage threat ranking model depended on attack timeline, called: The Palpation, Permeation, Perpetuation the three stages, explained in Fig.3.

Figure3: Explain security threats, ranking and attack timeline



The three stages of Security threats showed as followed:

- First Stage (Palpation): the initial phase or stage in threat attack time point to as the survey phase. At this phase weak network or systems are discovered via process as palpation. For instance, an attacker multi ports scan to find out and describe networks and different systems that are online to determine services, application and many processes implement on certain system, consequently, the social engineering cheating techniques may engaged to collect information about people or systems as part of the palpation stage.
- Second Stage (Permeation): the second phase in threat attack time, in which an attacker tries to cheating of security controls to make opportunities to create damage in the system. Consequently two sub-categories are distinguished: a) unauthorized access: include intentionally threatening (malicious and deliberate) attempts to bypass access through control mechanism to cause damage and predispose

different systems to damage. For instance, dictionary and brute force attacks: b) (DoS) Denial of Service: that occurs when the threats do not need authorized access breaking or cause damage a system for malicious and deliberate damage. For instance networks snooping, computer worms, (DDoS) Distributed Denial of Service attacks and (DoS) Denial of Service distinguished by the try to comprehensively damage different resources required to transfer services to alleviate legal users.

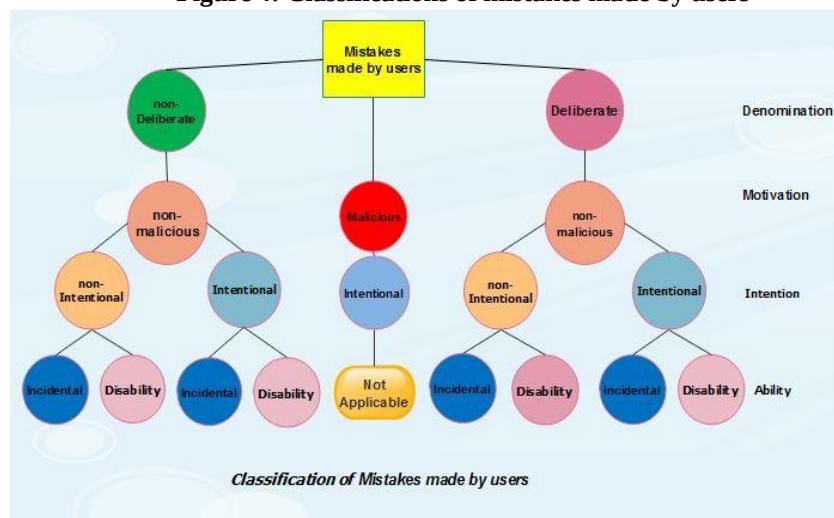
- Third Stage (Perpetuation): This third stage in which threats have successfully penetrated via system or network illegally for malicious intentions. In this stage four sub-categories are included: a) Detection of data and information: occurs when the intent reveal for system or information and data, then breaching of system .b) Doctrinaire of data: occurs with intent to alter data and information or system leading to disadvantage of the integrity data and information or system. c) Demolition of system or data: abused of integrity occurs when the internet is to demolish possessions. D) Removes traces: the attacker seek to cleaning- up traces of attack to prevent legal discovery evidence to avoid crime or prosecution, Tipton et al. [12]. Different precautionary measures are required at each stage of the attack timeline. For instance, at the first Stage (palpation) host and network based on obtrusion detection systems are necessary and required to reveal port scans. It is explain importance of this stage to successful attack as showed. United States Army's Field Manual 100-5 operation, Heagney et al. [18], stated success attack depended on accuracy of the scouting. While the Second Stage (Permeation), the control mechanisms and robust access also required together with (DoS) denial of service alleviation tools. For instance, success authentication, license, different accounting mechanisms, firewall and (DoS) alleviation tools. The third stage (perpetuation), different effective forensic medical tools connected with effective monitoring systems for networks. Eventually, each stage is important and required of the timeline different alleviation controls. Subsequently, these classifications regarding security threats of attack timeline relevance to equip effective and timely precautionary measures to threat than categories that examine weaknesses regardless misunderstand of threat diffusion dynamics.

B. Classification of Threats

Different threads faces up computer network or whether was portable or stable devices networks form outside or inside of the institution including: breaching, cyber-threats (terrorism), threads by disgruntled some employees and environment threads such as (flooding, earthquakes or wildfire) according to, Talbi et al. [4, 17]. Generally, the threads environmental or human-made threats cause's faults in systems in terms of Development and Interaction via network and these threads unintentional and intentional demonstrated in Fig.4. However, threads causes damage to hardware systems or hardware content and affecting equipment performance and all operation system such as incorrect operation, penetrationsystem to distortioninformation or accidental system shutdown. These classifications are used to evaluate and intent of threats. For instance,

- Network faults (such as errors in systems design) are caused by non-deliberate, non-malicious and accidental human actions such as ease password help authorized person sign in to system.
- Intentional software threats (such as links leads to viruses or computer worms), are caused deliberately and malicious, by deliberate human-action.
- Multi Cyber-threats (such as terrorist attack to breaching or destroy the system) or insiders 'threats (such as disgruntled person) all these threads are caused through intentional, malicious or deliberate human actions.

Figure 4: Classifications of mistakes made by users



V. Conclusion

Managing threats and weaknesses for (EEs) is challenging and very difficult, because increasing number of weaknesses incidents in possessions. In this respect, organizations need to protect their valuable possessions from penetration or unintentional errors caused by human actions to reducing associated hazards to their possessions. Threats should not order how functions of organization are run. Therefore, threats can be an obstacle to this; and prevent availability of information to legal person. This article explains, how adequately manage both weaknesses and threats that invest weaknesses in possessions. The precautionary measures are require to execute convenient work; but this is only accessible through models that catch the potential to inclusive represent what needs or that best protect valuable possessions to be protected. The contributions in this article are involves objectives in managing securityfor EEs; aimed primarily at providing comprehensively regulations and frameworks to organizations that help fully understand requirements in managing security, such as, i) what needs to be protected (valued possessions), ii) being control to suitably classify them, iii) assessing weaknesses within classified possessions ,iv) determine threads that exploit weaknesses),v) evaluating the hazard to possessions as an outcome of threads and weaknesses.vi) eventually, , recommending to increasing of precautionary measures. In addition, execute protection controls like penetration detection systems or firewall and anti-virus if factors (i-vi) have not be evaluated by and determined. Take into account the finance factor in managing Emerging Enterprises (EEs), it work on minimal financial budgets for security if compared to other enterprises. This factor is convincing and recognized in this article via model proposed as well as some security facets collected thereby reducing capital costs in (EEs) of both management and implementation. However, in this article the model distinguish capabilities multiple security issues if compared to models that addresses specific in this scope and isolated security issues, end up this article explained a comprehensive process in managing security for (EEs).That examines threats, weaknesses and hazards to computer networks and devices associate with network to provide adequate precautionary measures in protecting valuable possessions of an organization.

V. References

- [1] M. E. Whitman and H. J. Mattord, Principles of information security: Cengage Learning, 2011.
- [2] A. M. Khalfan, "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors," International Journal of Information Management, vol. 24, pp. 29-42, 2004.
- [3] M. Whitman and H. Mattord, Management of information security: Nelson Education, 2013.
- [4] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," University of California, Berkeley Report No. UCB/EECS-2010-5 January, vol. 20, pp. 2010-5, 2010.
- [5] Y.-P. Ou Yang, H.-M. Shieh, J.-D. Leu, and G.-H. Tzeng, "A VIKOR-based multiple criteria decision method for improving information security risk," International Journal of Information Technology & Decision Making, vol. 8, pp. 267-287, 2009.
- [6] Y.-P. O. Yang, H.-M. Shieh, and G.-H. Tzeng, "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment," Information Sciences, vol. 232, pp. 482-500, 2013.
- [7] A. D. Basha, S. H. Mnaath, I. N. Umar, and R. Jamaludin, "Insight on Protection of Universities Networks Information Security: The Problems and the Solutions," 2013.
- [8] S. H. Mnaath, A. D. Basha, R. Jamaludin, and I. N. Umar, "Devices of Computer Network Security and Visualization Control System: Design and Implementation," 2013.
- [9] B. L. Williams, Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2. 0, and AUP V5. 0: CRC Press, 2013.
- [10] W.-H. Hsiao, H.-K. Su, Y.-S. Wei, W.-S. Ho, and K.-J. Chen, "A Study of SLA-Based Defense Resource Management Strategy in Network Security Defense System," in IFIP International Conference on Network and Parallel Computing, 2012, pp. 336-348.
- [11] S. Liu and Y. Fang, "Application research in computer network security evaluation based on genetic algorithm," in Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on, 2012, pp. 468-470.
- [12] H. F. Tipton and M. Krause, Information security management handbook: CRC press, 2003.
- [13] H. Susanto¹², M. N. Almunawar, and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," International Journal of Electrical Computer Sciences IJECSEJENS, vol. 11, pp. 23-29, 2011.
- [14] H. Susanto, M. N. Almunawar, Y. C. Tuan, M. S. Aksoy, and W. P. Syam, "Integrated Solution Modeling Software: A New Paradigm on Information Security Review," arXiv preprint arXiv:1204.0240, 2012.
- [15] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level," International Journal of Engineering and Technology. IJET Publications UK, vol. 2, 2012.
- [16] H. Susanto and M. N. Almunawar, "Information security awareness within business environment: An it review," 2012.
- [17] I. Ruuska, K. Arto, K. Aaltonen, and P. Lehtonen, "Dimensions of distance in a project network: Exploring Olkiluoto 3 nuclear power plant project," International Journal of Project Management, vol. 27, pp. 142-153, 2009.
- [18] J. Heagney, Fundamentals of project management: AMACOM Div American Mgmt Assn, 2016.
- [19] M. Vanhoucke, Measuring time: Improving project performance using earned value management vol. 136: Springer Science & Business Media, 2009.
- [20] M. Vanhoucke, Integrated Project Management and Control: Springer, 2014.
- [21] J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security: CRC press, 2016.

VI. Acknowledgments

I would think organizations in collection some facts regarding their works and regards to University of Sumer – Department of Computer Science & Information Technology, to help in publishing my paper.