Available at: www.sabauni.net/ojs

# S.J.I.T.N

# Saba Journal of Information Technology and Networking

**Available at: www.sabauni.net/ojs**

S.J.I.T.N
Saba Journal of
Information Technology
and Networking

## *Advisory Board*

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of
Information Technology
and Networking

# Contents

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

REVIEW STUDY

# WEB DECISION SUPPORT SYSTEMS: TECHNOLOGIES, MODELS, AND SECURITY

*Arwa Y. Aleryani*
*Faculty Of Computer And Information Technology, Saba University*

**Article info**

**Article history:**

**Accepted Mars, 2016**

**Keywords:**

**Web-based DSS Definition**

**Architectures and technologies**
**Models and implementations**

**Security**

## Abstract

New technologies, especially the world-wide web technologies, have created many opportunities for effective Decision Support Systems. Web- based DSS provides an efficient tool that helps users find information resources available as an online service within an Intranet.

This paper reviews key topics which concentrate on technical issues of Web Decision Support Systems (DSS) research. It highlights the potential results from various papers and researches on Web-Based Decision support system. Our aim is to focus on Web-based Decision Support System definition, architectures and technologies, models and implementations, and Security.

* Corresponding author: Arwa Y. Aleryani
E-mail address: Arwa_y@hotmail.com

A decision support system (DSS) is a computer program application that explores and analyzes many sources of related data and presents it so that users can make decisions more easily. The main challenge of Decision Support Systems is to improve the quality of decision-making and the performance of decision makers [**1**]. The advances in computer technologies have impacted everybody's daily life as computers support and assisted almost every single human activity. Traditional decision support systems (DSS) focus on computerized support decisions with respect to managerial problems [**2**]. Web-Based DSS take advantage over traditional DSS, where it makes use of widespread Web technologies to distribute the decision making process among a various group of geographically dispersed end- users, many traditional DSS implementations were controlled by localized client/server systems [**1**]. Researches in the decision sciences have resulted in the development of a variety of Decision Support Systems (DSS) that are useful in solving many decision problems faced by individuals and organizations. It is now possible to access these DSS using the Internet. However, it is often difficult for individuals and organizations to locate specific DSS that could benefit them. Nowadays, the Internet provides access to thousands of gigabytes of information, with more information being added every day [**3**].

## Theoretical Background

The Decision making process starts with the intelligence phase, where, potential problems and/or opportunities are identified and defined. In the design stage, alternative solutions to the problem are developed. In the choice stage, a specific action is chosen. In the implementation stage, action is taken to put the solution into effect. In the monitoring stage, the implementation of the solution is evaluated to determine if the expected results were achieved and it modifies the process.

DSS applications can be composed of the following subsystems [**4**]: (1) Data Management subsystem: The database management subsystem includes a database, which contains relevant data for the situation and is managed by software called, the database management system (DBMS). The database management subsystem can be interconnected with the corporate data warehouse, a repository for corporate relevant decision-making data. (2) Model Management subsystem: The model base gives decision makers access to a variety of models and assists them in decision making. The model base can include the model base management software (MBMS) that coordinates the use of models in a DSS. (3) Knowledge-based Management subsystem: This subsystem can support any of the other subsystems or act as an independent component. It provides intelligence to augment the decision maker's own. It can be interconnected with the organization's knowledge repository, which is called the organizational knowledge base. (4) User Interface subsystem: it allows users to interact with the DSS to obtain information. The user interface requires two capabilities; the action language that tells the DSS what is required and passes the data to the DSS and the presentation language that transfers and presents the user's results. The DSS generator acts as a buffer between the user and the other DSS components, interacting with the database, the model base and the user interface.

## Literature Review

**Tripathi [4]** attempted in his paper to highlight the decision support system as a tool for making the better decisions in the organization. The researcher has proposed the study with respect to Birla Corporation Limited. **Tripathi** studied the "Attendance Recording System (ARS)" at Birla Corporation Limited. The main objective of Attendance Recording System is to ensure that the attendance of employees is accurately recorded and reported for computation of payable days, overtime hours, festival allowances, payable assistance etc. This automated system helps managers and employees to save their time and improve their work. By eliminating manual record keepings, it reduces errors, avoiding arguments. The DSS (designed in this study for Attendance Capturing & Recording for Birla Corporation Limited) mainly generates the reports like Daily Attendance, Monthly Attendance, Sick Reports, etc. The top management, by receiving these reports, can analyze and make decisions regarding shifting the priority of the job, also the observance of performance and corrective measures are taken. The author came up with that DSS, developed specifically to help managers to keep control on the staff's work at various levels. The Reports generated are as per the format which will help top management to make decision concerned with human resources in attendance recording and capturing, which is one of the basic needs of any organization. The Decision Support System is required for managerial report generation specialized tools; software and procedures are used to develop DSS in the organizations.

**Valentin,** et al. **[5]** presented in their paper an original model of an information system for decision making, which is able to provide reliable management solutions in various fields. They presented some overviews of the proposed decision support system and then exposed three cases where it has been successfully applied: two applications in university management and one in urban planning. Their proposed model has shown that the decision support system allows the decision maker to choose the best alternative out of a set of possible interventions, based on a group of custom-defined criteria. The developed algorithm requires good mathematical abilities from the user, and this can therefore limit the real-life applicability of the proposed decision support system. In order to make it easier for the users to use the DSS and increase the number of potential users, the DSS was implemented online with a user-friendly interface.

The purpose of their approach is to offer a set of tools to the decision makers by leaving the computational part to the server. It allows users to concentrate on planning issues rather than having to understand the formulae that lie behind the algorithm. The results of this paper; which are obtained using the proposed information system in the three cases presented in the paper, show its high flexibility and the usefulness of information systems for management.

**Yao [2]** viewed Web-based Support Systems (WSS) as a multidisciplinary research area that focuses on supporting human activities in specific domains or fields based on computer science, information technology, and Web technology.  His paper presented the fundamental issues of WSS, a framework of WSS, and research on WSS. He also presented preliminary studies on two examples of WSS, Web-based research support systems (WRSS) and Web-based information retrieval support systems (WIRSS). **Yao** concluded his paper that emerging interdisciplinary study of Web-based support systems is motivated by the challenges and opportunities of the Web. He indicated that the research of Web based support systems is a natural growth and extension of existing research. The evolution of the application dimension is the extension of decision support systems to computerized support systems. With the emergence of Web technology and Web intelligence, various Web-based support systems are extended from a single machine to a single user computerized support system. Finally he showed that there are four types of existing research, namely, WSS for specific domains, Web-based applications, techniques that are related to WSS and design, and the development of WSS that can be classified as WSS research.

**Shim** et al. [6] discussed the evolution of DSS technologies and issues related to DSS definition, application, and impact. They presented four powerful decision support tools, including data warehouses, OLAP, data mining, and Web-based DSS.

Issues in the field of collaborative support systems and virtual teams are presented. The authors also described the state of the art of optimization-based decision support and active decision support for the next millennium. Finally, some implications for the future of the field are discussed. They arrived to the fact that a standard Web browser can be used as the user interface/dialog, that means that companies can introduce new DSS technologies at their sites at a relatively low cost when compared to client-based DSS. Only a little user training is required with Web browser user interface at implementation of DSS technology

**Chien-Chih** [7] due to the rapid advancement of electronic commerce and web technologies in recent years, the concepts and applications of decision support systems have been extended a lot. One quickly emerging research topic is the consumer-oriented decision support system that provides functional supports to consumers for efficiently and effectively making personalized decisions. **Chien-Chih** presented an integrated framework for developing web based consumer-oriented intelligent decision support systems to facilitate all phases of consumer decision-making process in business-to-consumer e-services applications. His paper resulted that through using the consumer-oriented intelligent decision support system (CIDSS), all phases of the consumer decision-making process can be supported, and in addition, serving consumers with great satisfaction may eventually lead to continuing consumer relationships as well as add values and assets to the entire value chain. He argued that major application functional modules involved in the system framework include consumer and personalized management, navigation and search, evaluation and selection, planning and design, community and collaboration management, auction and negotiation, transactions and payments, quality and feedback control, as well as communications and information distributions.

**Rosso** et al. **[**1] discussed the DSS Capabilities Deliverable over Web. Web-based DSS can deliver a huge number of decision support platforms. Among these are Data-Driven DSS, Model-Driven DSS, Optimization DSS, Communication-Driven DSS and Knowledge-Driven DSS. The two most common of these are Data-Driven and Model-Driven. Data-Driven DSS refer to a DSS system that allows the access to and manipulation of data. Their report has sought to outline the usability of the Web and the unique enabling technologies that power the Internet. They reported that, there are many benefits of web-delivered DSS tools, like reduced costs, universally accepted communications infrastructures and ease of use. That has established Web-Based DSS as the preferred platform for the delivery of information to facilitate effective decision-making. In the same time they reported that security is still an important concern.

**Okleshen** et al. **[8]** their paper highlights the potential of Customer Decision Support Systems (CDSS) to assist students in education-related decision making. These resources can be employed by faculty to effectively advice students more on various elements of college life. In the same time students can use them to participate more actively in their own learning and improve their academic experience. The authors also summarize consumer decision support systems (CDSS), concepts and benefits. Students can make use of these websites to support their education-related decision making. The authors discuss the potential benefits and drawbacks such resources create from a student perspective and conclude with directions for future research.

The benefits of CDSS that provide insights into consumer choice processes, increase customer loyalty, and reduce marketing costs. In addition, if the faculty recommends such systems to students, it is more likely they will generate greater student satisfaction and confidence with the advising experience (i.e., service encounter) and the decisions that ensue. On the other hand, their disadvantages include high costs, slow inquiry response time, and the difficulties posed by mediated learning formats, as well as ethical issues. They ended their paper is to illustrate the potentially valuable role of customer decision support systems may perform in assisting students with education-related decision making. Professors and personnel at all institutional levels can use these resources to advise students within all areas of college life, while students can refer to them individually when facing specific challenges.

**Gregg** et al. [3] inducted in their paper that the explosion of information on the World Wide Web

(WWW) and on corporate Intranets has made it increasingly important to have methods of organizing and understanding the available content. Their paper focuses on verifying a metadata model designed for distributing decision support systems (DSS) over the Web.

Metadata is one method that is being used to facilitate both, the location of specific Web content and the assessment of its quality. It is the information about the structure and content of a data resource and it allows businesses and consumers to locate appropriate resources and judge their power.

## Web-based Decision Support System Definition

Decision Support Systems can be defined as computer technology solutions that can be used to support complex decision making and problem solving [**9**]. A DSS is defined as a system that "assists management decision making by combining complicated analytical models and tools, and user-friendly software into a single powerful system that can support semi-structured or unstructured decision making"[**8**]. One of the most significant advancements of Web-Based DSS, in contrast to traditional DSS implementations, is the ability of ordinary customers and “casual users” to make use of information generated by these tools [**1**].

Some of the most significant weaknesses of traditional DSS systems include the high cost involved in the implementation and maintenance, and a dependence “on expensive IS resources for widespread use.” Web-Based DSS goes a long way in eliminating these concerns.

Global access to Internet resources, the well-known and user- friendly browser interface, and the relatively low costs involved in implementation make Web-Based DSS a step closer to the ideal of paperless e-business management [**1**]. Web-based systems are regarded as “platforms of choice” for delivering decision support while taking into account many technical, economic and social considerations [**9**].

## Architectures and technologies

Beginning in the early 1990s, four powerful tools emerged for building DSS. The first new tool for decision support was the data warehouse. The two new tools that emerged following the introduction of data warehouses were On-Line Analytical Processing (OLAP) and Data Mining. The fourth new tool set is the technology associated with the World Wide Web [**6**].

A Web-based DSS uses the Web as a portal to the underlying DSS. It lets users access and make use of the underlying DSS through the Web [**9**]. Web technologies have provided a new media for sharing information about decision support and a new means of delivering decision support capabilities. For DSS developer, the big leap forward is to use the “web as computer” [**10**]. A number of enabling technologies have evolved in just the last ten years. That facilitated the distribution of DSS services over the Web. Among these is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of Internet standards [**1**].

## Models and implementations

As decision making moves from an individual activity toward a group activity, many organizations are creating ‘‘virtual teams’’ of geographically distributed knowledge workers to collaborate on a variety of workplace tasks [**6**]. Distributed implementation of the underlying DSS is important for a Web-based DSS and presents a challenge, which needs the combination of a DSS with distributed computing technology [**9**]. E-commerce makes use of the decision support system. It plays an important role on its application. The benefits of using a decision support system in e-commerce adoption includes improved customer service, better inventory control, and lower marketing and distribution costs, reduced cycle time, increased market reach, and reduced operation costs [**11**]. Metadata Model is the description of the structure of the database in database environment. It is used to describe the structure of the files, the type and storage format of the data, and the constraints on the data. Metadata are used in the Web environment to identify the content and quality of Web pages. The Open DSS protocol metadata model currently includes functional attributes related to the problem domain of the DSS, the solution options, the inputs, the outputs, and the assumptions made. The Open DSS metadata model also includes metadata on the resources required to execute the DSS. Information on the hardware requirements (e.g., computing platform), software requirements (e.g., operating system or application needs), and any specific user skills required to use the DSS are all included. Finally, the metadata model contains all other information necessary to purchase and download the DSS. This includes information on the DSS’s cost, its references, related DSS, and source/author information [**3**].

## Security

There are three main security items to keep in mind when selecting a Web tool that permits access to crucial data: First, it should be compatible with your existing firewall and encryption layers. Second, it should use caching wisely in a security-conscious manner; and finally, it should manage passwords for optimal safety and convenience [**1**]. There are at least four systems that perform some or all of the web-based DSS. The four systems are Joint Protection Enterprise Network (JPEN), Joint Warning and Reporting Network (JWARN), Area Security Operations Command and Control (ASOCC), and Protect, Respond, Inform, Secure, and Monitor (PRISM). A description, overview, and summary of each system’s capabilities will follow [**12**].

## Conclusion

By reviewing various papers and researches on the Web-based Decision Support Systems, we can conclude that the web is where the DSS action is today. It is obvious and clear that DSS provides valuable information required for making effective and efficient decisions where it cannot be ensued without the information pool such as the Internet. Also World-Wide Web technologies have rapidly transformed the entire design, development and implementation process for all types of

Decision Support Systems. This new environment allows individuals and organizations to make more informed, more collaborative decisions that will help achieve the organization's goals more effectively. The developments in the last decade will guide us in understanding the coming growth of decision support technologies. The implementation environment users are becoming more sophisticated and more demanding, and organizations are becoming more complex. These are some of the future challenges which have to be deeply researched and investigated. Finally the computer science and web technology will not stop at any point, they will both continue to grow up and develop new inventions constantly.

## References

[1] Rosso, M., Randolf, P., Rodrigues, K. (2001) "A Report on Web-Based Decision Support Systems" , California State University Fresno, Available via http://marosso.tripod.com/mba253/dss.pdf

[2] Yao, J. T., (2008), An Introduction to Web-based Support Systems, Journal of Intelligent Systems, Vol. 17 No.1-3, pp267-281, available via http://www2.cs.uregina.ca/~jtyao/Papers/JIS_WSS08.pdf

[3] Gregg, D. , Goul, M. , Philippakis, A. (2002) "Distributing decision support systems on the WWW: the verification of a DSS metadata model" , Elsevier Science, Decision Support Systems 32 (2002) 233– 245

[4] Tripathi, P. (2011) "Decision Support System is a Tool for Making Better Decisions in the Organization" , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2 No. 1

[5] Valentin, G., Calin, D. (2013) " Considerations Regarding the Flexibility of Information Systems for Decisional Support", Annals of the Constantin Brâncuși University of Târgu - Jiu, Engineering Series, Issue 4/2013

[6] Shim, J.P., Warkentin, M., Courtney, J. F., Power, D. J., Shard, R., Carlsson, C. (2002) "Past, present, and future of decision support technology Decision Support Systems" 33 (2002) 111 –126, Published by Elsevier Science B.V.

[7] Chien-Chih Yu, " A Web-Based Consumer-Oriented Intelligent Decision Support System for Personalized E-Services", Supported in part by National Science Council under Project NSC 92-2416-H004-019, Available via http://nccuir.lib.nccu.edu.tw/bitstream/140.119/26465/1/p429-yu.pdf

[8] Okleshen, C. , Bradbard, D. ; Martin, M. (2005 ) "Customer Decision Support Systems: Resources for Student Decision Making" , The Journal of Educators Online, Volume 2, Number 2.

[9] Bessedik I., Taghezout N. (2006) "A Multi-agent Framework for a Web-based Decision Support System Applied to Manufacturing System" , University of Oran

[10] Bhavgave, H., Power, D. "Decision Support System and Web technologies:

Status Report" available via http://dssresources.com/papers/dsstrackoverview.pdf

[11] Velmurugan, M , Narayanasamy, K. (2008), “Application of Decision Support System in E-commerce” , Communications of the IBIMA , Volume 5

[12] MAJ Gregg Powell, COL Charles Dunn III. “ Homeland Security: Requirements for Installation Security Decision Support Systems” available via https://cryptome.org/2013/06/dhs-prism.pdf

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

## Article

# FRAME DUPLICATION FORGERY DETECTION USING PHYSICAL RANDOM OBJECTS

*Tawfiq S. M. Barhoom *, Ahmed J. I. Elaff*
*Information Technology Faculty, Islamic University of Gaza*

**Article info**

**Article history:**

**Accepted Jan, 2016**

**Keywords:**

**Digital Tampering**

**Digital Forensics**

**Image Forgery**

**Frame Duplication**

## Abstract

Due to the revolution of image editing video tools, it is easy to tamper with any video by altering, combining or creating new video contents. A common way of manipulation is to duplicate frames to hide objects. We proposed a new reverse algorithm to discover the duplication of the frames to stop theft by stopping the ip-cam in specific places.

* Corresponding author: Tawfiq S. M. Barhoom
E-mail address: tbarhoom@iugaza.edu.ps

## Introduction

In the last few years, many social media sites were published to enable users around the world to share their knowledge, life events and their diaries. This makes a huge amount of data that is replicated to be used for defamation. One of the types of media is videos and the tampering with them, which makes the privacy of the internet and its contents less confident.

However, the problem lays on the tampering process before sharing these resources. These videos have turned to be harassment to some people. Another problem is tied to the network resources that are being hacked and edited before publishing.

The video forgery or tampering has two types: Active and passive [1,2,3], the active allows the user to make watermark [4,5]or signature to the videos before publishing and when it is being tampered with, we check the watermark or signature for any editing or changing. This type is rarely used because we can't know if the video really needs to do that or not, and in the online recording system that decreases the performance of the recording frames speed. Another approach is a passive one which means to check the video by several techniques with several purposes such as reversed algorithm. We can detect the changes by a sensor device pattern [6, 7] or reverse post-production techniques such as white balancing. When the DETECTOR finds any changes in the video content the DETECTOR detects that it has been tampered with. The other ones are duplication on regions and frames to hide an object or change its position or make the duplication increase the object number which is used in wars to increase the objects of rockets or military equipment.

In recent years, due to the improvement of network technologies and devices, IP-cam is a device that is connected to the networks to watch the places we want to with low-costs and expenses.

One of the problems of this device is related to connecting it to the network all day. So if any attacker hacks this LAN, this device will be driven by the attacker and will be turned off. The attacker can show any video regardless if the IP-cam is tied to the system or not. One of the attacks is to change the checking system of the video with duplication of frames to hide the thief's personality. And with a corporation with the thief he can steal or ignore the cam recording process.

In this paper we proposed a new method called DETECTOR. The DETECTOR has been added between the video and the system alarm to detect the duplication by using a random animation object. We can compare the frames to ensure that they are no duplicated regions in the specific area in efficient way.

Our methodology includes multiple steps to make this process more efficient such as using Grayscale to speed up the image processing in our online system.

In this paper we will also discuss the process with details, results and evaluation with all measurements taken for the online camera and offline videos.

## Related Work

### *Video Inpainting Forgery Detection Techniques*

“Inpainting is the process of reconstructing lost or deteriorated parts of images and videos. For instance, in the case of a valuable painting, this task would be carried out by a skilled image restoration artist.”[8]

Here inpainting is used to remove objects by filling the gap with adjacent pixel colors as shown in Fig. 1. The difference here is our purpose and usage. Here it was used to hide objects but in our research, we used it to detect frame group duplications to ensure that the video has not been edited.

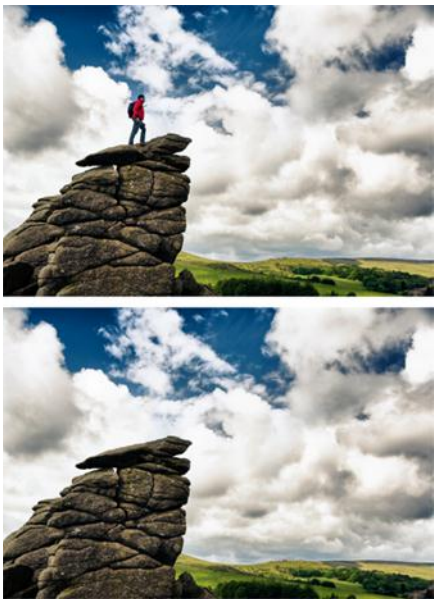


*Fig. 1: The top figure shows a character is that hidden in the lower picture by inpainting*

### *EXPOSING DIGITAL FORGERIES IN VIDEOS BY DETECTING DUPLICATION*

It’s a paper that talks about how to detect region and frame duplication. Regarding the frame duplication, we can see this example by looking at Fig.2.The figure shows a series of videos captured by the cam of a man who is moving through the camera in the top series but at the bottom the frames are duplicated to hide this person. Compression techniques were used to convert the frames to JPEG instead of PNG ones to make the comparison faster.[11]

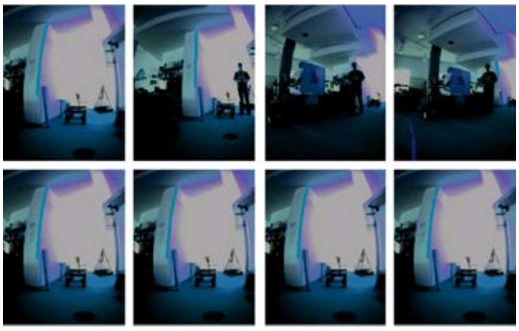


*Fig. 2: The top figure shows a sequence that show a person and in the bottom one the person is hidden by duplication*

Here the tampering (hiding objects) was discovered by checking the repeated frames that were duplicated to hide an object. In our research we do the reverse. We want to check the duplication of our physical object. When the duplication is found with the motion we can detect the duplication where it needs less image processing and faster because we only check the region that the physical object lies on and not whole frame.

### *ADOBE Premiere Pro CC*

Adobe Premiere is a program used for video editing and montage for multiple videos. One of the features of the new version called CC, is used to check duplication series in editing processes and not in the full rendered and extracted ones. So it used to check the video duplication in the editing process which is called active forgery and that type is not useful for criminal investigation.

Fig. 3 shows the duplication detecting done to check the colour series. If it's similar that means it is duplicated.[12]

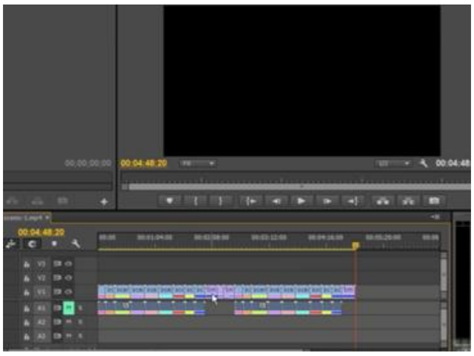


*Fig. 3: Duplication detected by watching the similar colours means that this frame is duplicated*

## System Architecture

In this section we have defined the system components and where the DETECTOR is actually located. The component of the system is an IP-camera for recording the video which is connected by a hosting hardware system to store the recording video through the camera. When there is any problem, the hosting system monitoring software starts the alarm system to close the doors and make a loud sound to inform the police. Our DETECTOR lies between the system that records frames (which can be hacked and store the forgery video) and the alarm system as shown in Fig.4.to check the frames; as we will discuss in the next section. Then if there is a forgery of duplication, the alarm system starts working

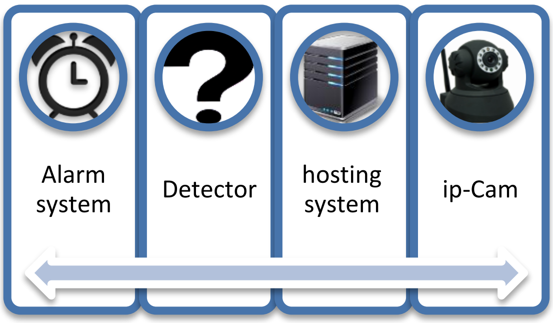


*Fig. 4: The components of the system and where the DETECTOR lies*

## Methodology and Implementation

This paper's experimental implementation is programmed on HTML5. This is a powerful language to handle the pixels and change their colour system, such as grayscale. Not needing to add plug-ins, and good for making image processing online because it handles the video as the image to make processing on it.

The DETECTOR has been tested on different multiple offline videos and online webcams to make a sense of the minimum resolution needed, and the frame rate to make the process faster and efficient.

Before making any process, a random animated object which is animated randomly without animation repetition period will move in specific region in any corner in the camera boundaries it can be a digital clock including the date to ensure that no repeating in the days periods or something else, so the detection will be in this region to ensure that it's not repeated. Our methodology is based on seven steps, as shown in Fig. 5.

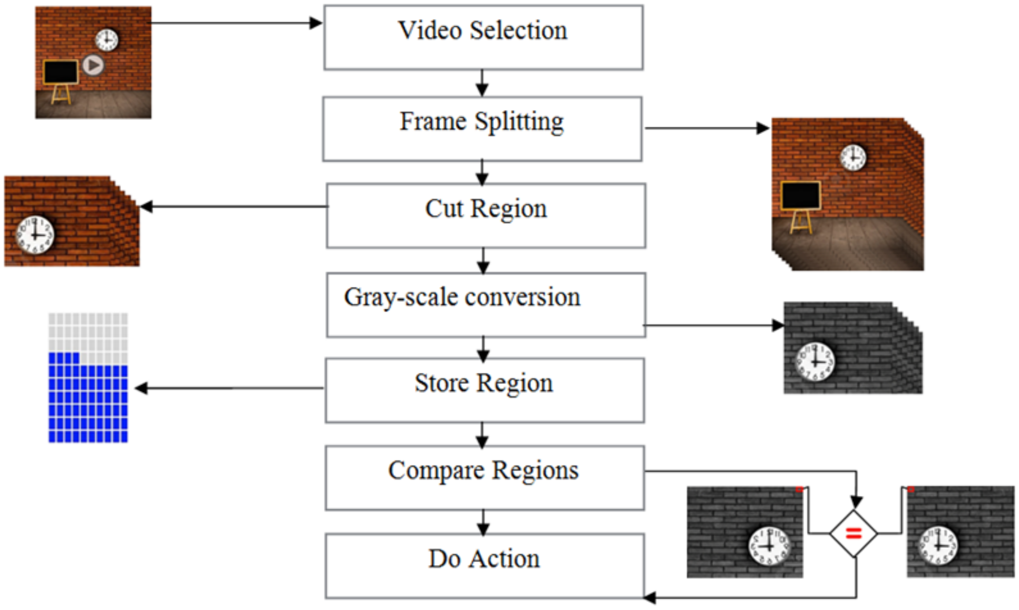


*Fig. 5: methodology processes*

You can follow these steps to detect the frame duplication forgery:

- ***Video Selection:***

Our experiment is based on taking a number of offline videos to detect if they were tampered with or not. We used a multiple of videos with deferent properties such as different dimensions, multiple colours and different frame rates. And the next step is to apply it by an online IP camera

- ***Split to frames:***

- Because the pixel processing cannot be performed on all the video, we are concerned by the duplication on frames. So we must split the video taken to frames. We didn't mean to take all the video to achieve the performance, but we checked the duplication for multiple random series of frames.

- ***Cut the region:***

Cut the region that contains the physical object to make the process more efficient unless you take all the frames together which we needn't, the process becomes faster.

- ***Grayscale Conversion:***

Convert the taken regions to grayscale unless the RGB makes the process faster.

- ***Store the region:***

Store the regions in the array and sort as the frame sequence in the video.

- ***Compare regions:***

By taking the stored regions and compare their pixels, after a specific amount of time we can detect the duplication.

- ***Do Action:***

Here we detect if there is a duplication region or not. However, if there is duplication, we can do any action such as turn the alarm on or calling the owner's number.

## Experiment Measurements

In this paper, the DETECTOR has been tested for 3 videos where each video is a 2 minutes long. The first one contains one duplication frame every second. The second video has 20 duplication frames distributed randomly. And the last one has no duplication frames. Every video has a 400x600 dimension with a 24 fps frame rate. We tested these 3 videos on the DETECTOR and the error percentage was zero. But the challenge was the time which the DETECTOR has consumed and which was 20 to 40 second for 2 minutes, it depends on the pixel density and the resolution number of the video.

Before the pre-processing grayscale conversion technique, the DETECTOR took approximately 3 times more than now, and if we look to the region comparison, it reduced more time and which can be computed from the following equation:

$$T(Region) = \frac{\text{region } width \ \times \text{region } height}{original\ width \ \times original\ height} \times \rho \times 100\%$$

T(Region): the time the DETECTOR does consume for regions.

$\rho$ : the pixel density percent. If the pixels are focused on this region, it will make a variance.

The DETECTOR has been developed in HTML5 JS language which is powerful in color correction to make grayscale, cropping the regions and pixel comparison moreover than it can be used for online cameras as we talked about in the introduction.

## Conclusion

In this paper, we have proposed a digital video forgery detection scheme using a random animation object that moves in the camera boundaries. We proposed a 3rd party system between the watching systems and the alarm one to detect the camera stopping or what we called frame duplication. We are using an HTML5 for it is powerful for handling the video as an image and looping on its pixels to make the changes to grayscale. Cutting the regions and comparing the pixels DETECTOR is fast and efficient because it checks regions on grayscale with powerful language.

## References

[1] Deshpande, P., & Kanikar, P. (2012). Pixel based digital image forgery detection techniques. IJERA, 2(3), 539-43.

[2] Chittapur, G. B., Murali, S., Prabhakara, H. S., & Anami, B. S. (2014). Exposing Digital Forgery in video by mean frame comparison techniques. InEmerging Research in Electronics, Computer Science and Technology (pp. 557-562). Springer India.

[3] Johnson, M. K., & Farid, H. (2006, September). Exposing digital forgeries through chromatic aberration. In Proceedings of the 8th workshop on Multimedia and security (pp. 48-55). ACM.

[4] Hsieh, C. T., & Wu, Y. K. (2006). Geometric invariant semi-fragile image watermarking us-

ing real symmetric matrix. WSEAS Transaction on Signal Processing, 2(5), 612-618.

[5] Lin, P. L., Hsieh, C. K., & Huang, P. W. (2005). A hierarchical digital watermarking method for image tampers detection and recovery. Pattern recognition, 38(12), 2519-2529.

[6] Khanna, N., Mikkilineni, A. K., Chiu, G. T., Allebach, J. P., & Delp, E. J. (2007, February). Scanner identification using sensor pattern noise. In Electronic Imaging 2007 (pp. 65051K-65051K). International Society for Optics and Photonics.

[7] Chen, M., Fridrich, J., Goljan, M., & Lukáš, J. (2008). Determining image origin and integrity using sensor noise. Information Forensics and Security, IEEE Transactions on, 3(1), 74-90.

[8] Das, S., Darsan, G., Shreyas, L., & Devan, D. (2012). Blind detection method for video inpainting forgery. International Journal of Computer Applications,60(11).

[9] Bayram, S., Avcıbaş, İ., Sankur, B., & Memon, N. (2006). Image manipulation detection. Journal of Electronic Imaging, 15(4), 041102-041102.

[10] Patwardhan, K. A., Sapiro, G., & Bertalmio, M. (2005, September). Video inpainting of occluding and occluded objects. In Image Processing, 2005. ICIP 2005. IEEE International Conference on (Vol. 2, pp. II-69). IEEE.

[11] Wang, W., & Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In Proceedings of the 9th workshop on Multimedia & security (pp. 35-42). ACM.

[12] Detect Duplication Frames Automatically | Adobe Premiere Pro CC [Online]. Last access : 11-2-2015 , Available : https://helpx.adobe.com/premiere-pro/how-to/premierepro-duplicate-frame-detection-cc.html

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

## Article

# METHODS OF SAFEGUARDING THE SITES FROM SQL INJECTION

*Muneer A. S. Hazaa*, Muneer Ali Saif Algabry, Mahmoud Mahub Qaid Altayar*

*Thamar University Faculty of Computer Science and Information System*

**Article info**

**Article history:**

**Accepted Jan, 2016**

**Keywords:**

**Structure Query Language (SQL)**

**Injection Attacks**

## Abstract

Due to the rapid expansion of internet, web applications have become a part of everyday life. Consequently, this has increased the number of web application incidents and exploits web application vulnerabilities. For that consider the SQL injection type of attacks that target web applications and allows attackers to obtain unauthorized access to the backend database to change the intended application-generate.

* Corresponding author: Muneer A. S. Hazaa
E-mail address: muneer_hazaa@yahoo.com

## Introduction

SQL injection is considered to be one of the simplest types of attacks in nature and the most dangerous for web applications.  There are a lot of Website developers who do not realize the nature of the attacks and therefore many of them do not perform the simplest of preventive measures to protect databases they are dealing with against the impact of these attacks. This gap is considered to be common in most of the Websites and through which most of the websites are penetrated and quite important   data gets stolen. In this paper, we will focus in the first section on how this gap happens and how to address it. In the second     part, we will focus on how to raise the protection level of the site for the prevention of pirate attacks by hackers. [1] Thus, we will focus on a big problem in websites. This study makes it open for other researchers to study other problems in sites.

## Methodology

The authors used programmable functions (see section 2) that codify the password through making it pass through many levels in a way as to make it much more complex for hackers to execute their plans. Such functions are so useful in making webs much safer. We also used a program to discover all the gaps (see section 5).

### *Research Problem*

There are programmable gaps by SQL injection in the websites that make them accessible for hackers. So, such gaps need to be detected and countermeasures should be made to save the websites.

### *SQL Injection*

Query Language injection is to add symbols and SQL statements to the variables that are passed as parameters for the query where  these sentences are implemented  with the underlying query and then the attacker can have unauthorized    access to  the system databases and retrieve sensitive information-on from databases .[2]

Attacks pose greater risk due to the fact that they impact databases which are critical to any organization. [3]

### *Background on SQL injection vulnerability*

Many people say they know what SQL injection is, but all they have heard about or experienced are trivial examples. SQL injection is one of the most devastating vulnerabilities that has a great impact on a business; as it can lead to exposure of all of the sensitive information stored in an application's database, including handy information (such as usernames,  passwords, names, addresses, phone numbers, and credit  card details).[4]

### *Examples of realistic breakthroughs caused by the SQL gap*

Among the institution breached banks are PNC Bank Nasdaq Stock Exchange, Heartland Payment Systems and many others, which led to losses estimated at hundreds of millions of dollars suffered by these companies. The interesting thing is that these people carried out the break through on a long period of time from 2005 until the time of their arrest in 2012.

According to the source, they use these gaps in SQL databases to enter them and then install some of the codes, that allow them to enter through a back door to private networks of such institutions breached the time they want .They have been able to obtain data on the numbers and more than 160 million bank account Credit Cards through that process. [5]

***Some major hacks regarding SQL injection [7]***

- July 2012, Yahoo confirms 4 million accounts hacked.

-June 2011, Hactivist 'Lulzsec' breached the website of SONY.

-May 2011, COMODO Brazil got breached

-March 2011, Official homepage of MySQL website was compromised.

-November 2010, Royal Navy website was attacked

-January 2009, Heartland payment systems got breached.

-June 2007, Microsoft UK website was defaced.

***Preventing SQL In Existing Applications***

SQL injection issues are relative new in the information security area. Many old systems were designed when developers were not aware of such threats. In fact, SQL injection vulnerabilities are so prevalent that simple Google searching can find many of them. To rewrite all of the vulnerable code sections of an existing system is both time-consuming and often impractical due to financial or time constrains. Therefore, techniques for protecting deployed systems against SQL injection attacks are important.

[8]This part will present how to protect our gaps SQL. We must follow the following:

***Screening and matching input variables in terms of the type and length***

We must examine any input before passing it to the query sentences. Let's say we want to display data for a product, according to the product number and the imposition of the latter part of the link would be as follows:

index.php? cat = 20

As seen at the link above, there is a variable called cat value that was passed as 20 and this value will definitely query in a table of products supposing that the query is as follows:

Select * from category whereid_cat = '$ cat'

Select * from category whereid_cat = '20 '

As noted in the previous query that the value of the variable cat has been passed to the query without any examination of the data contained before passing it by the attacker. The attacker could exploit this vulnerability to pass other values for the implementation of other queries such as

20 '+ union + select + * + from + category + order + by + '1';

index.php? cat = 20 '+ union + select + * + from + category + order + by + '1'

The query will be as follows:

We note here that the database category table or spreadsheet or others have been queried and the attacker can pass other queries to view other data or executing orders that harm the site. This happens because of the lack of screening examination though the input examination is simple and we can address the former gap as follows : Since the value of the variable cat will be passed, the value to the field id_cat whose data type is digital .We can receive its digital value as follows:

$ cat = intval ($ _GET ['cat']);

The Previous function intval receives the variable values cat on the grounds that it is numeric values . Therefore any text that enters, the function ignores it and maintains only the number .Even if the data entered is a text, it will become zero.

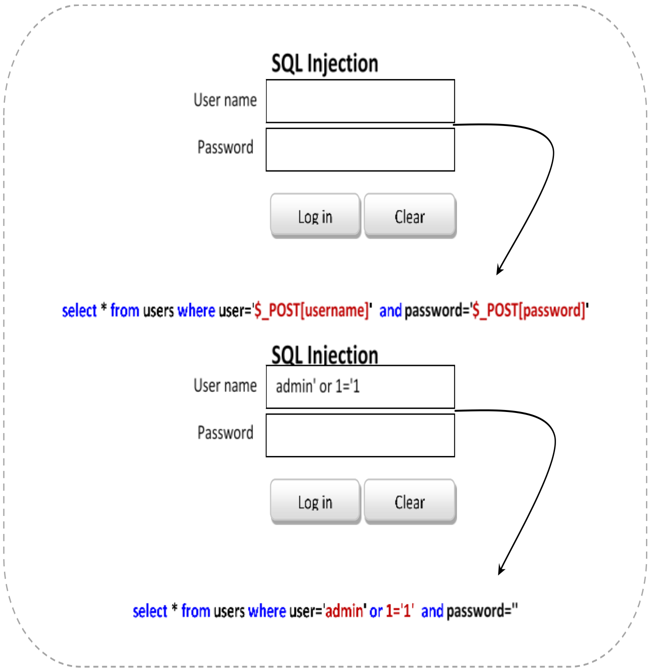
We use this method with the variables of numeric type, while with the variables that receive text values , we must pass these values on one of the functions that add mark / before Marks ' or' and it will be as follows:

$ cat = mysql_real_escape_string ($ _GET ['cat']);

We can also test the length of the variable before passing them by the attacker. For example, if the length of the variable is 20 characters, we will receive the value of the variable only to the limits of twenty symbols as follows:

$cat=mysql_real_escape_string (substr($_GET['cat'],1,20));

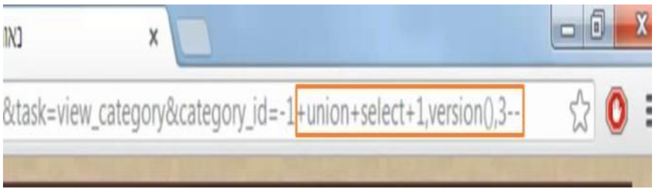
Example for SQL Injection Show in Figure1



```
select * from users where user='$_POST[username]' and password='$_POST[password]'
```

```
select * from users where user='admin' or 1='1' and password=''
```

*Figure 2 show how can pass a query by attacker in the bar.*



```
&task=view_category&category_id=-1+union+select+1,version(),3--
```

*Figure 2. Pass a query union in the web site a bar.*

***Error messages (Hide)***

Site programmer must hide error messages that appear when there is an error in the site so as not to be exploited by the attacker.

For example, we can adjust the settings file php.ini to prevent the emergence of error messages by controlling the following characteristic.

display_errors = off

log_errors = on

***We*** can also work messages prepared in advance in order to appear for the user in case any error may occur.

<? Php

$ cat = intval ($ _GET ['cat']);

```
$ sql = "select * from category where id_cat =". $ cat;
$ q = mysql_query ($ sql) or die (" Unable to execute the query because of erroneous input ");
?>
```

We also note that the above-mentioned function of Die has been used to display a message when there is an error in the implementation of the query.

We can also use the @ sign before the name of the function to avoid the appearance of error messages.

***Encoding Passwords Using More Than One-Way Function.***

Encrypting passwords in the database using unidirectional encryption as follows,

If the encryption function here is by using md5,

The decryption is not impossible. But when we encrypt the password using the overlapping encryption, the encryption would be very strong.

Example:encryption password by more than function is as follows:

```
<?php

$pass=sha1(mysql_real_escape_string(strip_tags($_POST['pass'])));

echo "Leve 1 : ",$pass,"<br>";

$pass=sha1($pass);

echo "Leve 2 : ",$pass,"<br>";

$pass=md5($pass);

echo "Leve 3 : ",$pass,"<br>";

echo "Leve 4 : ",md5(sha1(sha1(mysql_real_escape_string(strip_tags(($_POST['pass'])))))),"<br>";

?>
```

In this way we have made the password encryption as difficult as possible and the more the multiplicity of levels of encryption the more difficult the decryption is.

For example: if we encrypt (muneer), the password encryption levels will be as follows:

Level1:
1c2c0fef3c4f1b85f97db36724a08eb291ce6d84
Level2:
07e1bdb71b98487a181245275efaff2e1be89052
Level3: e1aaf499a7be62f4a5aa586801906470
Level4: e1aaf499a7be62f4a5aa586801906470

As we have seen above, the password encryption has become strong. If the penetrator tries to decode this code e1aaf499a7be62f4a5aa586801906470, it will appear for him after a huge effort as follows: 07e1bdb71b98487a181245275efaff2e1be89052

Thus, this is not the decoding of the encryption and so we have increased the difficulty of decryption. If the penetrator arrived to the database and got the password, there will be several levels of difficulty ahead.

***Hiding Of Variables That Appear In URL***

As we have seen previously, SQL injection is passed through the URL addresses so that we can hide the variables that are passed by titles by concealing links and converting them into html by

Mod rewriter in order to limit the penetration site via a URL.

Using the file: we can perform this by using Htaccess. The code will be as follows:

URL Rewriting with PHP

http://www.apache.org/BookDetails.pl?id=5

You could provide a filter which accepts URLs such as http://www.apache.org/Book/page5.html

The following is what needs to go into your htaccess file to accomplish that:

Rewrite Engine on.RewriteRule ^ Book/page([09]+)\.*(html*)$BookDetails.pl?id=s 1

Note: to activate this characteristic, we must go to the file httpd.conf,and #LoadModulere-write_module modules/mod_rewrite.so

We remove # sign and it becomes in this form: LoadModulere-write_modulemodules/mod_rewrite.so

Hence, the feature is activated.

Note: Must be enabled Mod_rewrite.

LoadModulere-write_modulemodules/mod_rewrite.

### *Put A Fire Wall On The Control Panel Folders*

To protect the folders, we must first logon the control panel of the site through C Panel. http://www.website.com/cpanel

Figure 3 shows protect folders Control Panel.

### *Password Protected Administration (Htpasswd)*

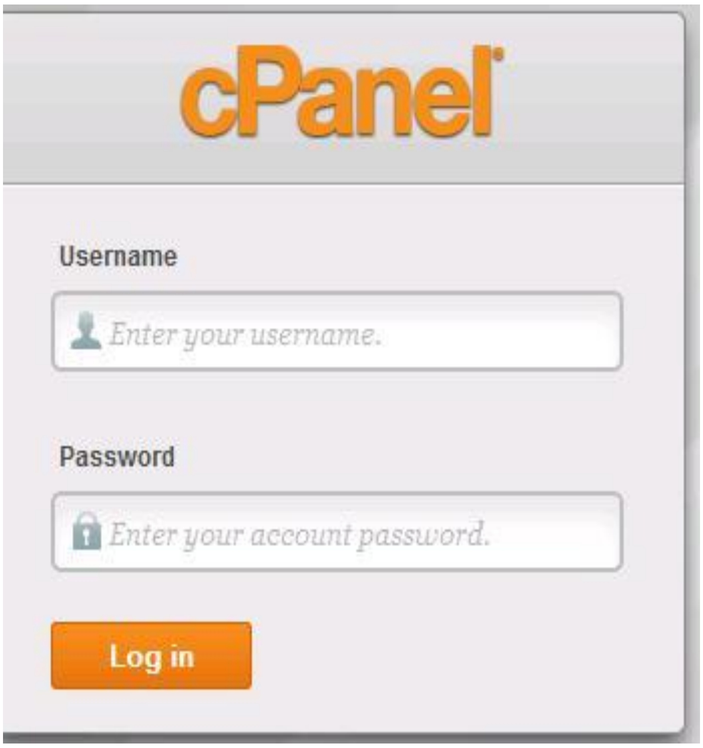


*Figure 3, Login Control Panel.*

We write the username and the password and then click on login which has in previous figure3.

The control panel appears as figure 4.

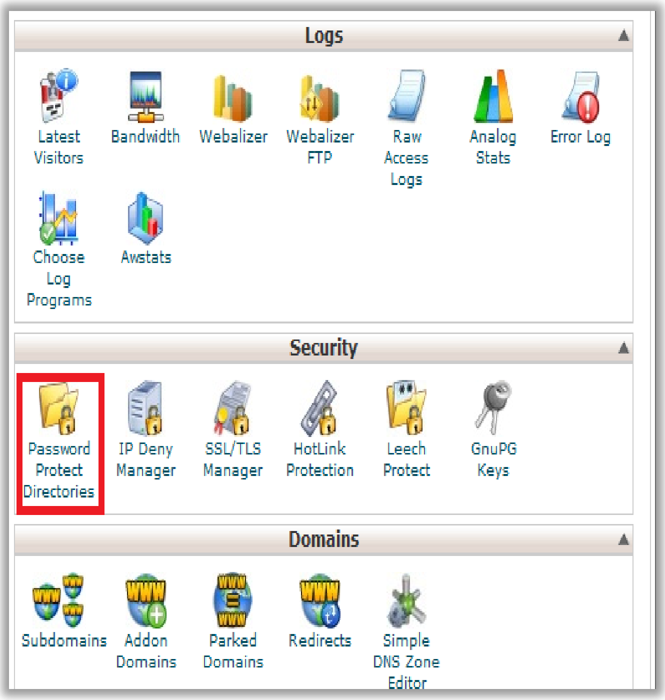
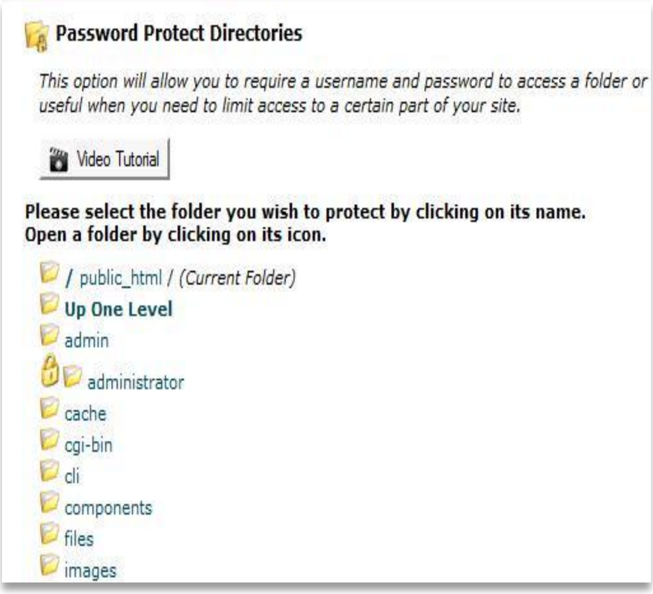


*Figure 4, Protected Directory*

From the previous window we click on Password Protect Directories to appear as shown in the following *figure:*



**Password Protect Directories**

*This option will allow you to require a username and password to access a folder or useful when you need to limit access to a certain part of your site.*

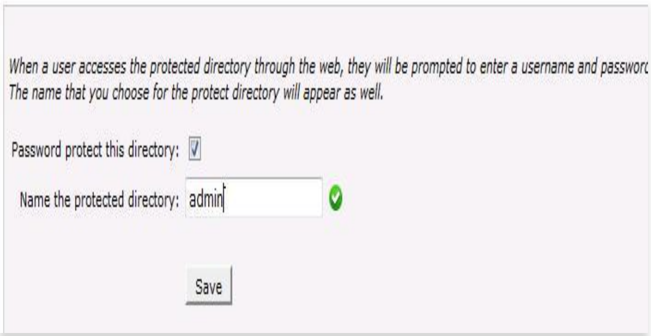
Video Tutorial

**Please select the folder you wish to protect by clicking on its name. Open a folder by clicking on its icon.**

- / public_html / (Current Folder)
- **Up One Level**
- admin
- administrator
- cache
- cgi-bin
- cli
- components
- files
- images

*Figure 5. Password protect Directories*

From the previous window we click on the name of the folder that we want to protect for, example the folder Admin, to appear the window as shown in figure *6:*



*When a user accesses the protected directory through the web, they will be prompted to enter a username and passworc The name that you choose for the protect directory will appear as well.*

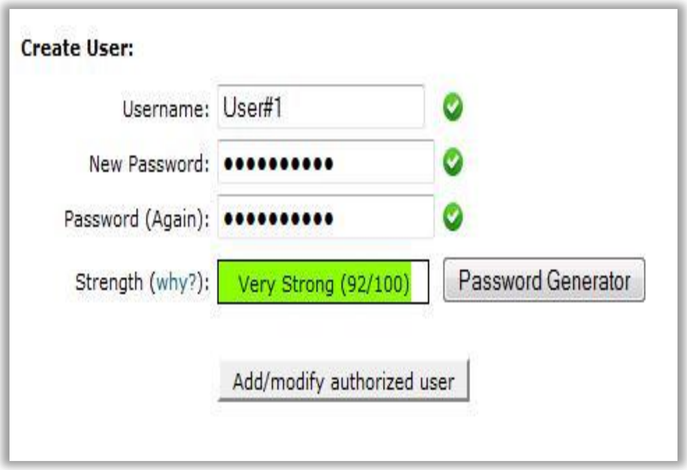
Password protect this directory: ☑

Name the protected directory: admin ✓

Save

*Figure 6. Protected directory*

From the previous window, we write the name of the folder that we want to protect and then click on Save.



**Create User:**

Username: User#1 ✓

New Password: •••••••••• ✓

Password (Again): •••••••••• ✓

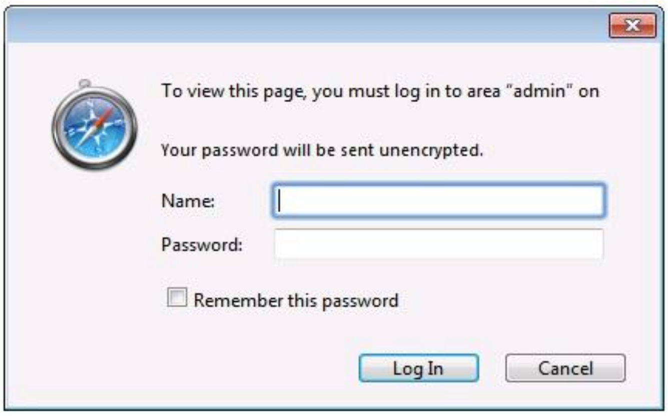
Strength (why?): Very Strong (92/100) Password Generator

Add/modify authorized user

Figure 7, Add or Modify Authorized User

From the previous (figure 7), we create a user name and a password, and then we click on the button Add /modify  authorized user for protecting the folder of management with a password .When you attempt to access the Management folder , the  firewall window appears as following figure :

http://www.website.com/admin



To view this page, you must log in to area "admin" on

Your password will be sent unencrypted.

Name:

Password:

□ Remember this password

Log In Cancel

*Figure 8, Access to the Management Folders*

We have thus put a firewall on the control panel of management to ensure that access to the Management folder is not easy. Also, we would better choose an uncommon name for Management folder , that is ,we  change the management folder name to numbers and names which are difficult for the hackers to guess .

### *Change Paths and Names of Folders Control Panel*

Methods of protection task are to change the names of folders and paths to the control panel so that it is difficult for the hacker to guess them. We should not give the Management folder names that are commonly known. Such as Administrator, Admin, manager, user, control, login, log, Cpanel, panel,

We must give them names that are unknown and difficult to guess by hacker programs that are used in the process of guessing For example, we can name the Management folder as d3xcs08e better than to give it the name Admin. After giving it an unknown name, we should also protect it with a firewall. It is also better to create folder names for known names to the control panel. Such as admin and administrator and make these folders empty and set up the firewall so as to delude the penetrator that this is the control panel so as not try to search for the real folder of the Control Panel.

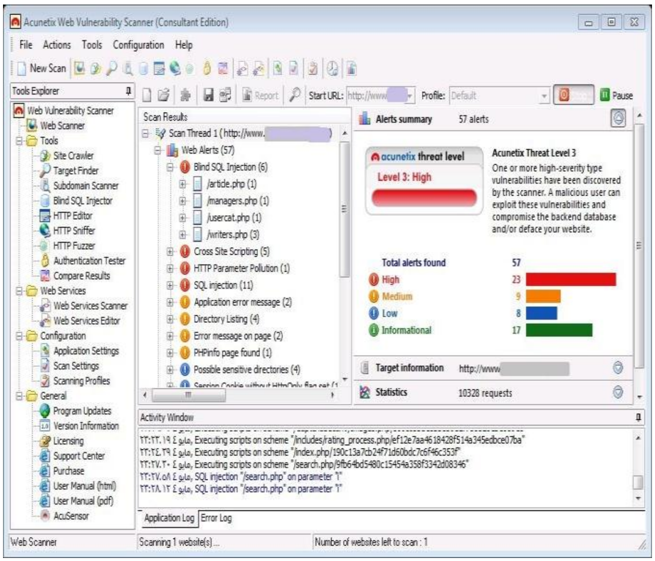
### *Prohibition of Visitors Who Pass On Codes of Injection Queries*

Useful ways to prevent the hacker from targeting a site is blocking the site when the error message of the prevention of injection process appears. We record the IP address of the visitor that caused the error and when the error is repeated more than twice or three times. For example, we block the site for the visitor for an hour so as to avoid the process experience injection thread by hackers. This is an effective way to prevent the pirates from trying to experiment on the target site.

### *Web Vulnerability Scanner*

Vulnerability Scanner scans your web application for vulnerabilities. We used a program called ***Acunetix vulnerability scanner*** to scan the web application in a way as to show all kinds of gaps (see figure 8).This helped us to discover the dangerous gaps by which the hackers get an unauthentic access to the backend databases. Therefore, we can make protection for such applications. The program can be used this way easily:

Open Web application and click “Scan Site" for whole site scanning or "Scan URL" only for current URL.



Scan Thread 1 ( http://www.[redacted] )
Web Alerts (57)
Blind SQL Injection (6)
/article.php (1)
/managers.php (1)
/usercat.php (1)
/writers.php (3)
Cross Site Scripting (5)
HTTP Parameter Pollution (1)
SQL injection (11)
Application error message (2)
Directory Listing (4)
Error message on page (2)
PHPinfo page found (1)
Possible sensitive directories (4)
Session Cookie without HttpOnly flag set (1

57 alerts

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

| Total alerts found | 57 |
|---|---|
| High | 23 |
| Medium | 9 |
| Low | 8 |
| Informational | 17 |

Target information http://www[redacted]
Statistics 10328 requests

```
٢٢:٢٣.١٩ ٤ مايو, Executing scripts on scheme "/includes/rating_process.php/ef12e7aa4618428f514a345edbce07ba"
٢٢:٢٤.٢٩ ٤ مايو, Executing scripts on scheme "/index.php/190c13a7cb24f71d60bdc7c6f46c353f"
٢٢:٢٧.٣٠ ٤ مايو, Executing scripts on scheme "/search.php/9fb64bd5480c15454a358f3342d08346"
٢٢:٢٧.٥٨ ٤ مايو, SQL injection "/search.php" on parameter "i"
٢٢:٢٨.١٢ ٤ مايو, SQL injection "/search.php" on parameter "i"
```

Web Scanner | Scanning 1 website(s) ... | Number of websites left to scan : 1

Figure 9, Web Vulnerability Scanner

## Conclusions and Recommendations

This section includes the most important conclusions of this research.

In this research, we found that the intrusion protection requires a re-examination of the site, and programming to address the gaps in it. Moreover, it is found that developing several levels of protection on the website is required even if the first level exceeded breach collide at the second level and so on .In this research, we found that choosing a hosting company, which provides powerful means of protection on the part of the server is important, in addition the level of security at the sites needs to be improved after the addition of the levels of protection mentioned in this research. There are many gaps that were not mentioned in this research so it is not sufficient to address the gaps mentioned, but you should search the rest of gaps and address them.

Means of protection that have been mentioned in this research are not considered as 100% efficient for protection because there is no 100% protection. The field is broad and it is pirated everyday so we must always search for the latest attacks and innovate new means of defense to make it more difficult to be hacked. Finally, detecting and blocking attacks against known vulnerabilities is required. The knowledge base of exploitable weaknesses in the application must be frequently updated

## References

[1] Center of Excellence for Information Security.

[2] A Survey on SQL Injection attacks, their Detection and Prevention Techniques *V. Nithya, IJECS Volume 2 Issue 4 April, 2013 Page No. 886-90*

[3] Mittal, P. (2013). A Fast and Secure Way to Prevent SQL Injection Attacks using Bitslice Technique and GPU Support (Doctoral dissertation)..

[4] SQL Injection Attacks and Defense 2009 Justin Clarke Lead Author and Technical Editor.

[5] Department Of Justice http: //www.justice.gov/opa/pr/2013/July/13-crm-842.html

[6] History of SQL Injection”[Online].

Available: http: //hackertarget.com/10-years-of-sql-injection.

[7] DARK SIDE OF SQL INJECTION ASAR International Conference, Bangalore Chapter- 2013, ISBN: 978-81-927147-0-7

[8] A Survey Of SQL Injection Countermeasures. June 2012. Dr. RP. Mahapatra and Mrs. Subj Khan

Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

Article

# Examining the Impact of Privacy, Security and Legal Framework on Trust in Mobile Computing in Business Environment: An Exploratory Study

*Qais Hammouri *,Emad Abu-Shanab , Ahmad Manasrah*
*IT College, Yarmouk University, Irbid, Jordan*

**Article info**

**Article history:**

**Accepted Jan, 2016**

**Keywords:**

**Security**

**Privacy**

**Trust**

**Law**

**Mobile computing expert opinion**

## Abstract

With the vast and rapid growing of information technologies, the use of mobile computing has increased dramatically. This led to the emergence of concerns related to information security, customers' privacy, guiding laws, and lack of trust in using mobile services. This study will investigate the issues related to trust in mobile computing and its impact on users of mobile devices. The results demonstrated that both privacy and security are essential issues that affect users' trust and hence, the adoption process. Results also indicated that an adequate legal framework that governs security issues needs to be developed and enforced in mobile computing and business environments. The detailed results of this study are reported with conclusions at the end.

* Corresponding author: Qais Hammouri
E-mail address: hammouriqais@yahoo.com

## 1. Introduction

Mobile technology has grown significantly over the past few years. A wide range of mobile technologies became available for users like smart phones, tablets (PCs), notebooks and laptops. Two important phenomena emerged: First, great computing power of Smart phones along with its place convenience. Such feature encourages the development of many new mobile applications offered to users online via the app store. The second phenomenon is the spread of malware, which is increasingly deployed to extracting users' data. Nevertheless, effective mechanisms of defense are developed against malware because of the complexity of m-applications and their operating system (Santos, 2013). Using open networks such as the Internet environment, issues concerning trust and security become critical. The physical view of the network vs. the distributed nature and the user authentication concept to the domain is becoming more important. Kagal (2001) asserted that with the growing complexity of mobile devices in the modern era, the security of such devices (in the presence of countless attacks) is becoming the main issue. The majority of mobile phones are still not guaranteed against the existing and emerging security threats. Regardless of its nature, security attacks on mobile devices aim mainly at causing a system malfunction or leak of personal information (Mal-Sarkar & Bhunia, 2010).

Mobile computing provides users with a platform of information management system that is free from temporal and spatial constraints. Freedom from these restrictions allows users to access and process required information from any place and at any state (mobile or static). PCSs are connected to the Public Switched Telephone Network (PSTN) to provide access to wired phones (Kumar, 2004). Users of smart environment demanded solutions to be trustworthy, private, and secure. Security defines the techniques of cryptography utilized to secure required data and communication channels. Privacy is related to the risks involved in exposing personal information when interacting with ISs. Based on that, users' trust is defined in terms of users' allowed level of control on the quantity of information that could be disclosed, and the calculated risks or anticipated benefits that would stimulate users to share their information during such interactions (Nixon et al., 2004).

The general theory of confidence in computers and humans networks should be built on computational trust theory or behavioral trust theory. These theories depend on the increased people participation in the protocols of socio-economic and social networking. The effective participation of users in the protocols depends mainly on trust. Strict on-line protocol compliance verification is often not practical, where verification can cause user's inconvenience. Confidence is captured through the preferences of participants (such as betrayal aversion or risk), and their beliefs in the credibility of the participants in another protocol (Gligor, 2011).

## 2. Literature Review

The convergence between mobile computing and the Internet allows personalized access to online services anytime and anywhere. Such feature creates great opportunities for new business models that stimulate rapid innovation and vigorous investment. Unfortunately, such innovation produces also new threats and vulnerabilities, and the new business models also generate incentives for more attacks. The growth in mobile service and use of the Internet would face painful setbacks due to the unequal security measures and new emerging threats. The main factors to identity management sustainable development in online communities and markets were trust and security (Josang, 2013).

### *2.1 Mobile Computing Environment*

Handheld devices, such as smart phones, are becoming an increasingly essential part of human lives for communication, where their most convenient and effective benefit is that they are not bounded by place and time. Mobile users can benefit from diverse mobile applications like: Google Apps, iPhone apps, etc. With the rapid advancements in Mobile Computing (MC), there is a strong tendency to benefit from such phenomenon when joined by information technology. But, mobile devices face many challenges like its storage, bandwidth, battery life, and communication issues like security and mobility (Dinh et al, 2011).

At present, most of institutions utilized mobile devices at work to facilitate the services they provide and products they sell. Mobility enables employees to take their work with them wherever they go, including company proprietary information, sensitive customer data and intellectual capital data. Mobile devices enable employees to perform what they need to do, wherever and whenever they want. People could cooperate and collaborate in the field with business partners, customers, patients or students. Employees working in the field require data support for their transactions and processes like documents, Internet, or applications (Archer et al., 2012). Employees can access corporate resources using their mobile devices to increase their productivity and flexibility. But if their mobile devices are exploited or vulnerable, they become a source for leaking or corrupting crucial business information. Such benefit (company mobility initiatives) comes with cost; mainly risking the resources needed to manage the devices that contain the data and secure corporate data (Ro, 2012).

Data availability and increased connectivity provide new models for conducting business, but create new security risks. For instance, to simplify financial transactions, the organization may want to allow business partners or customers some accessibility to certain local resources. The institution should develop company policies outlining the privileges of extranet accessibility. Such relationship brings trust to the front page. Trust requires a repetitive detection of credentials among the two parties in order to build the needed level of confidence to complete any transaction (Winslett & Yu, 2001). Finally, improvements in MC device storage and power capabilities make the physical damage much more harmful to the organization. Additionally, they become attractive to profit-motivated cyber criminals (Robb, 2009).

Mobile phone users are divulging more information on their behavior and location on the basis of site data created when using their mobile devices. In criminal cases, law enforcement parties can access site data to help solve crimes; this confirms how data can be revealed in identifying patterns of individuals' behavior (Syme, 2009).

Mobility causes unplanned interactions among computer systems that are used by people to reach services in diverse environments. Before any transaction between two systems, systems must trust each other and satisfy the requirements of privacy and security (Caceres & Sailer, 2006). Mobile payment (M-payment) allows easy payment, thus, it has received considerable attention and became an important complement to the traditional payment methods. Nevertheless, m-payment via open networks makes security challenges more potent (Alafeef et al., 2013). Although much research has addressed security issues, still some security problems are not well resolved. An example is the problems of platform integrity and the protection of user's privacy. Authors have proposed public wage structure with trusted computing (TC) technologies to secure the m-payment transactions. Using simple infrastructure of mobile payment, a study presented a solution to protect the integrity of the platform, secure the payment software download, secure payment transactions, and protect application initialization (Zhong et al, 2009).

Huge market for mobile applications to serve e-commerce across the world is booming. Nevertheless, the demand for these services was challenged by privacy and security concerns of end users. The limited memory, limited processing of mobile devices, and its dependence on wireless channels made it inherently unreliable and left a little room for a layer of reliable security measures (Chaturvedi et al., 2013).

### *2.2 Trust and mobile computing*

The risks associated with mobile computing are increasing, where mechanisms, policies, and models are developed to assess the credibility of such service to each involved party. Trust formation depends on the reputation of the other party involved, recommendations from other users, or previous experience. Trust management allows for the recommendation of a service provider who is most probably to offer the necessary service whenever users are faced with a number of service providers who are not previously known (Seigneur, 2005).

People are increasingly saving more personal information on their mobile devices which increases the risk of losing such data or exposing it to unwanted people. The concerns of privacy and security in MC environment could be seen from different views including applications, user interfaces, databases, networks, operating systems and hardware (Khiabani et al., 2009). Threats against mobile devices are much more severe than conventional malware; mobile devices usually carry personal data more than desktop computers. Users may think that because they are carrying their mobiles constantly, they are securing them. But the physical control over the device does not necessarily guarantee the safe control of its content. Users have false security sense, which would lead them to a misleading confidence in such devices (Dagon et al., 2004). Mobile devices were developed to be lightweight and small, making it highly portable. Thus, they were susceptible to theft and loss. Mobile Devices could be protected through the use of smart cards and passwords. The types of trust in mobile devices reported in the literature are: trust of undercover-agent, trust of captured-agent, and trust of personal-agent (Mavridis & Pangalos, 2002).

Trust is an important factors influencing people’s adoption of any technology (Yan et al. 2009; Abu-Shanab, 2014; Khasawneh et al., 2013). Trust is the affirmative belief around the reliability, dependability and confidence in the process, object and persons related to MC services. When users are conducting transactions through mobile networks they are not likely to know the identity of service providers. In addition, mobile services collect information about users and their use behavior. Such process is bounded with ethical dimensions that require more attention, particularly ensuring user’s privacy (Kaasinen, 2005).

Trust in electronic transactions is developed by the "Trusted Computing Group" (TCG), which aims at imposing trustworthy conduct over computing platforms. The software chain consists of 'good software' like scanners for viruses. Such applications try to eliminate and identify harmful programs. The techniques suggested by "Trusted Computing Group" are concentrated around "Trusted Platform Module" (TPM). The TPM chip is connected to the Central Processing Unit-CPU and offers isolated storage for the keys of encryption and the 16 PCR "Platform Configuration Registers" (Lyle & Martin, 2010). When people use their computers they tacitly assume that their machines don’t include malware, like keystroke logger, and are not manipulated with. Such assumption is realistic because the unauthorized physical access to device is prohibited. For the vision of ISR (Internet Suspend/Resume), users should be capable of rapidly establish identical level of confidence in devices that do not manage or own. To tackle this problem, the Trust-Sniffer is created; a tool that assists users to gradually gain trust in un-trusted machines (Surie et al., 2007).

There are many behavioral and technical factors that influence the deployment and design of mobile applications. Trust is one of the main factors. In a study on confidence in an assortment of technology-based subjects like virtual teams and e-business, evidence is found that there is a need to ample trust for deployment of different computing environments. Consequently, it is also likely that confidence will be an important element in achieving successful deployment of computing environments everywhere (Valacich, 2003). Trust management or trust models within mobile environment need to extract standards for user's trust in various contexts, user's decision, feedback dissemination, and user's experience in trust or distrust. Nevertheless heterogeneity, uncertainty, and mobility of the mobile computing environment makes confidence management more complex, where users are becoming more undetermined, volatile, and mobile. The study suggested the model of distributed trust in the environment of mobile computing based on a range of useful notes about conduct of user (Wu, 2013).

### *2.3 Solutions for trust issues*

Trusted computing is expected to behave as expected by users. TCG promotes open standards to hardware enabled security technologies and trusted computing including software interfaces and across multiple devices, peripherals and platforms. It deploys a specified technology that enables computing environments to become more secure without affecting individual rights, functional privacy or integrity (Yan, 2007).

Kagal et al. (2002), suggested a solution for trust issues based on the management of distributed trust which includes thinking about the access rights of users, revoking rights, delegating trust to other parties, and developing security policy. The study depicted the infrastructure that supplement the existing features of security such as "Role Based Access Control" and "Public Key Infrastructure" (PKI) augmented by management of distributed trust to supply a high degree of flexibility for security in a widespread computing environment.

Security and trust issues were main factors in the deployment of cloudlet. The thick "Virtual Machine" VM boundary isolates a cloudlet from programs implemented by malicious or careless users. Nevertheless, a user's trust in the integrity of the infrastructure Cloudlet rests on assumptions that are more fragile. For instance, a malicious VMM can skillfully implement distortion of translation within the VM and consequently subvert a significant business deal without user being aware of harm (Satyanarayanan et al., 2009). The advent of deployed computing systems like Internet Resume/Suspend has facilitated the access to the personalized computing field of users through layers of "Virtual Machine" technology at the head of distributed storage. This model suffered from several challenges like establishing trust in unmanaged devices that users can access, and eventually migrating "Virtual Machine" (VM) state through networks of low-bandwidth (Surie, 2007).

### *2.4 Privacy issues in mobile computing*

Social networks are becoming more and more important as a popular platform for social interaction and communication between millions of users. Nevertheless, these systems pay little attention to the concerns of privacy and security associated with revealing friendship information and personal social networking behaviors (Beach et al., 2009). The protection of privacy through techniques of automatic anonymity is not bearable in which data richness and research value can be maintained at the same time. Trusted researchers are allowed to work with Lausanne Data Collection Campaign (LDCC) after accepting in written format to respect privacy and anonymity of the participants volunteering in LDCC (Laurila et al, 2012).

Policies related to privacy are confidence-based mechanisms that prescribe specific uses from location information. While regulations intend to provide group-based and global privacy guarantees, privacy policies intend to provide privacy protection that is elastic enough to adapt to the individual user's requirements and individual transactions. There are three key initiatives currently underway that described few methods to handle privacy issues and they are: Internet Engineering Task Force (IETF), GeoPriv, World Wide Web Consortium (W3C), Privacy Preferences Project (P3P), and Personal Digital Rights Management (PDRM) (Duckham & Kulik, 2005). In successful attacks on privacy, certain party gets unauthorized information. Persons can consent that certain information about them can be available for others, and other information should remain private. The key concern of privacy with respect to ubiquitous computing is that several vectors of automated attack become possible (Brandi & Rosteck, 2006).

### *2.5 Security issues in mobile computing*

Privacy and security are explored in most cases together when dealing with their importance to users and in mobile environment (Abu-Shanab & Ghaleb, 2012). Mobile cloud is combining cloud computing and mobile networks concepts. In mobile cloud computing the main challenges facing cloud services are performance, availability and security. Security of cloud computing is always the major factor and is ranked as a top priority for users and developers (Bahar et al., 2013; Sinjilawi et al. 2014). Cloud providers, mobile user, and other parties were all concerned about confidence. Basically confidence propensity is a personal trait. The reputation of service provider influences the level of confidence between the cloud and its clients. Standards required in the establishment of trust are the following: Security, privacy, robustness, stability, reliability, and elasticity (Sanaei et al, 2012).

Mobile cloud computing brings many advantages to hardware with minimum resources; benefits that lead to developing applications with rich functionality. Security issues in mobile cloud computing could be categorized into two major categories: cloud threats and mobile threats. The key purpose of these threats is to exploit the resources of mobile device or steal personal data (like location, calendar, contact database and passwords) (Popa et al, 2013).

Establishing applications on customized infrastructure rather than establishing applications on rigid and fixed infrastructure is offered by cloud computing. By tapping into the cloud, organizations benefit from adequate infrastructure resources and business applications with reduced capital expenditure (CAPEX). The cloud carries large size of information from enterprises and individuals, where security becomes more important (Ko et al, 2012). Security is associated with distribution, scale, concurrency, and multi-tenancy. Direct concerns originate from aspects like lack of control on code and data distribution at distributed infrastructures, and the loss of potential data. Also, the indirect issues originating from offering unlimited computational resources virtually to users raise the issue of trust by users (Kovachev, 2010).

## 3. Research Methodology and Results

### *3.1 Research model and hypotheses*

This research explored the research queries using two samples. The first sample filled a questionnaire exploring the descriptive of the items of survey. The second sample was used for the purpose of testing the model. The aim of the second sample is to investigate the main factors that influence the level of trust in mobile computing. Research model shown in Figure 1 depicts our premise in this study, where we hypothesize that security, privacy and legal framework will influence users trust in mobile computing. Similar premise was proposed by Al-sharafi et al., (2015), but in Internet banking area.

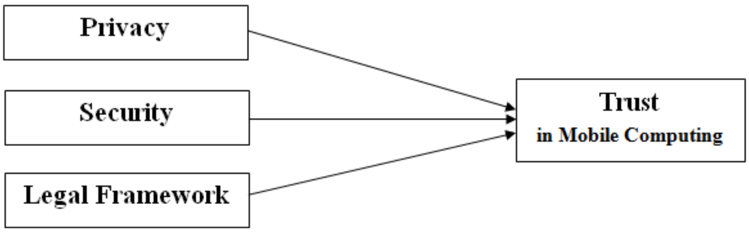


***Figure 1:*** *The research model*

The third factor proposed in this study is the legal framework, where previous research emphasized on the role of legal framework in defining the risks associated with technology (Abu-Shanab, 2012). This factor is not well researched and is considered a major contribution of this area. The following hypothesis is stated:

*H3: Legal framework existence will have a significant influence on Trust in Mobile computing.*

***The first sample:*** The developed survey was distributed to students in a public university in the Northern part of Jordan. The questionnaire focused on issues like: the existence of effective programs that cover privacy and trust in mobile computing, the effect of raising awareness to electronic security in mobile computing, and the existence of laws that protect privacy issues related mobile computing.

The questionnaire used utilized a 5 point Likert scale where 1 indicated a total disagreement, and 5 indicated a total agreement with the statements posted. The items covering the influence of privacy on trust were 5 as shown in Table 1. Similarly, 5 items measured security, 5 items measured legal framework, and 5 items measured the level of trust. The total sample size was 30, which is not adequate for relational statistical analysis, but benefited from the high awareness of graduate students where they might be considered experts in the domain. Research indicated that education level is a strong influencer of such domain (Abu-Shanab, 2011).

***The second sample:*** The same items were used in a second survey distributed after 6 months (based on the inadequacy of the first sample) but utilizing a 7 point Likert scale where 1 indicated a total disagreement and 7 indicated a total agreement with the statements posted. The total second sample size was 99 students, with 68 females (68.7%) and 31 males (31.3%).

***Table 1:*** *Survey items*

| | |
|---|---|
| **Privacy items** | |
| P1 | The use of mobile computing could reduce privacy. |
| P2 | Information exchanged among mobile computing devices has the necessary privacy. |
| P3 | The existence of effective programs that provide privacy when using mobile computing increases trust |
| P4 | Supplying users with the methods necessary to protect privacy increases trust in mobile computing. |
| P5 | The most important reasons for distrust in mobile computing is the lack of privacy |
| **Security items** | |
| S1 | The exchange of expertise in scientific and technological knowledge related to information security increases trust in mobile computing. |
| S2 | The use of mobile computing might reduce information security. |
| S3 | Providing the means of protection necessary to maintain security of information increases trust in mobile computing. |
| S4 | The most important reason for distrust in mobile computing is the lack of security |
| S5 | The awareness of electronic security could reduce IT crimes and increase trust in mobile computing . |
| **Legal framework items** | |
| L1 | The existence of adequate legal framework protects privacy and increases trust in mobile computing. |
| L2 | The existence of adequate legal framework supports security and increases trust in mobile computing. |
| L3 | The existence of adequate legal framework that punishes people who use mobile computing illegally will increase trust in mobile computing. |
| L4 | Trust in mobile computing is related to adequate legal framework |
| L5 | Legal framework has significant influence on mobile computing privacy and security issues |
| **Trust items** | |
| T1 | Awareness of mobile computing threats and how to avoid them increases confidence in mobile computing |
| T2 | Trust in mobile computing is affected by privacy degree. |
| T3 | Trust in mobile computing is affected by security |
| T4 | Trust in mobile computing is affected by legal issues |
| T5 | Trust in mobile computing leads to increasing its use. |

### *3.2 Data results and hypotheses testing*

This study depended on experts opinion regarding issues related to mobile computing security. In The previously mentioned questionnaire was distributed to 30 graduate students studying in a public university in Jordan. 53.3% of respondents were males, while 46.7% were females. Table 2 lists the frequencies of each item and the distribution of items in relation to the survey items mentioned in Table 1.

***Table 2:*** *Distribution of responses according to all survey items*

| **Privacy Scale** | **Privacy item 1** | | **Privacy item 2** | | **Privacy item 3** | | **Privacy item 4** | | **Privacy item 5** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| Strongly Disagree | 1 | 3.3 | 3 | 10 | 4 | 13.3 | 1 | 3.3 | 5 | 16.7 |
| Disagree | 6 | 20 | 9 | 30 | 4 | 13.3 | 2 | 6.7 | 3 | 10 |
| Neutral | 7 | 23.3 | 4 | 13.3 | 4 | 13.3 | 3 | 10 | 4 | 13.3 |
| Agree | 14 | 46.7 | 11 | 36.7 | 9 | 30 | 11 | 36.7 | 12 | 40 |
| Strongly Agree | 2 | 6.7 | 3 | 10 | 9 | 30 | 13 | 43.3 | 6 | 20 |
| Total | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 |
| **Security Scale** | **Security item 1** | | **Security item 2** | | **Security item 3** | | **Security item 4** | | **Security item 5** | |
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| Strongly Disagree | 0 | 0 | 2 | 6.7 | 2 | 6.7 | 4 | 13.3 | 1 | 3.3 |
| Disagree | 4 | 13.3 | 4 | 13.3 | 7 | 23.3 | 4 | 13.3 | 2 | 6.7 |
| Neutral | 3 | 10 | 3 | 10 | 0 | 0 | 0 | 13.3 | 1 | 3.3 |
| Agree | 15 | 50 | 11 | 36.7 | 10 | 33.3 | 13 | 43.3 | 12 | 40 |
| Strongly Agree | 8 | 26.7 | 10 | 33.3 | 11 | 36.7 | 9 | 30 | 14 | 46.7 |
| Total | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 |
| **Legal Scale** | **Legal item 1** | | **Legal item 2** | | **Legal item 3** | | **Legal item 4** | | **Legal item 5** | |
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| Strongly Disagree | 0 | 0 | 0 | 0 | 2 | 6.7 | 2 | 6.7 | 1 | 3.3 |
| Disagree | 2 | 6.7 | 1 | 3.3 | 1 | 3.3 | 1 | 3.3 | 1 | 3.3 |
| Neutral | 2 | 6.7 | 2 | 6.7 | 2 | 6.7 | 0 | 0 | 3 | 10 |
| Agree | 15 | 50 | 15 | 50 | 15 | 50 | 13 | 43.3 | 12 | 40 |
| Strongly Agree | 11 | 36.7 | 12 | 40 | 10 | 33.3 | 14 | 46.7 | 13 | 43.33 |
| Total | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 |
| **Trust Scale** | **Trust item 1** | | **Trust item 2** | | **Trust item 3** | | **Trust item 4** | | **Trust item 5** | |
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| Strongly Disagree | 0 | 0 | 2 | 6.7 | 1 | 3.3 | 0 | 0 | 3 | 10 |
| Disagree | 1 | 3.3 | 1 | 3.3 | 1 | 3.3 | 1 | 3.3 | 2 | 6.7 |
| Neutral | 4 | 13.3 | 8 | 26.7 | 7 | 23.3 | 5 | 23.3 | 8 | 26.7 |
| Agree | 13 | 43.3 | 12 | 40 | 15 | 50 | 15 | 50 | 15 | 50 |
| Strongly Agree | 12 | 40 | 7 | 23.3 | 6 | 20 | 9 | 30 | 2 | 6.7 |
| Total | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 | 30 | 100 |

The first step done on the second sample was to estimate the bivariate correlations between the variables and the means and standard deviation of each variable. Results are shown in Table 3 below. The results indicated a high perceived mean of each variable (all above 5). Also, a significant correlation was estimated between the variables and with an alpha value < 0.01. Finally, such result indicates that all three variables are important in influencing trust.

***Table 3:*** *Bivariate Pearson's correlations and the means and standard deviations*

| | Privacy | Security | Legal | Trust | Mean | Stand. Dev. |
|---|---|---|---|---|---|---|
| Privacy | 1 | | | | 6.2843 | 1.01568 |
| Security | .661** | 1 | | | 5.8530 | 0.98470 |
| Legal | .520** | .553** | 1 | | 5.7455 | 1.18729 |
| Trust in Mobile Computing | **.579**** | **.565**** | **.606**** | 1 | 5.6051 | 1.26145 |

**. Correlation is significant at the 0.01 level (2-tailed).

To test the hypotheses and the proposed research model we conducted a multiple regression test that regressed the three independent variables on trust in mobile computing. Based on that, the results indicated a significant model with an $R^2$ =

0.481, with an $F_{3,95}$ = 29.332, p<0.001. Such result indicates that the model explains 48.1% of the variance in trust in mobile computing. Finally, to know the influence of each variable on trust, the regression coefficient table shows such result. The results shown in Table 4 indicate a significant influence by privacy and legal framework, but not security.

***Table 4:*** *The regression coefficient table*

| Variables | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | -0.100 | 0.637 | | -0.157 | 0.876 |
| Privacy | 0.330 | 0.126 | 0.266 | 2.615 | **0.010** |
| Security | 0.240 | 0.133 | 0.187 | 1.799 | 0.075 |
| Legal | 0.387 | 0.097 | 0.365 | 3.982 | **0.000** |

*Dependent Variable: Trust*

## 4. Conclusion and Future Works

This research aimed at investigating the factors affecting user's trust in mobile computing environment. Two samples were used to explore the issues related to the research model proposed. A survey covering four dimensions was distributed among 30 graduate students (experts). The dimensions are: privacy, security, legal framework, and trust. Results demonstrated that both privacy and security are essential issues that affect users' trust to adopt and use mobile computing.

The use of mobile computing may also result in decreasing the security level for the transferred data; so users must be aware of the probable risks and threats that may occur in this environment. There must be also an adequate legal framework governing security issues to reliably transfer data in mobile computing environments. It can be also concluded that the exchange of the experiences between concerned authorities will result in improving the level of security and thus increase trust and the adoption of this technology. Future work is required to comprehensively explore the four dimensions and expand the sample size.

Furthermore, the same items but utilizing a wider scale (7 points Likert scale) and a different sample (99 bachelor students) was used to explore the relationships shown in the research model. Results indicated that 48.1% of the variance in trust can be explained by the data collected and by using privacy and the legal framework. The security factor did not predict trust as hypothesized. This result supports hypotheses H1 & H3, and failed to support H2.

This study drives researchers' attention to explore more the dimensions of security to understand why they did not compete well in the model. Also, our model supported the importance of the legal framework that covers mobile computing issues. This study suffered from the sample size in the first stage, where statistical analysis was not valid.

Also, using students in the second sample risks the generalizability of our conclusions.

## References

[1] Abu-Shanab, E. (2011). Education Level as a Technology Adoption Moderator.Proceedings of the 3rd IEEE International Conference on Computer Research and Development (ICCRD 2011). Shanghai, China, March 11-13, 2011, V0l 1, pp. 324-328.

[2] Abu-Shanab, E. (2014). Antecedents of Trust in E-government Services: An empirical Test in Jordan. Transforming Government: People, Process and Policy, Vol. 8(4), pp. 480-499.

[3] Abu-Shanab, E. &Ghaleb, O. (2012). Adoption of Mobile Commerce Technology: An Involvement of Trust and Risk Concerns. International Journal of Technology Diffusion, Vol. 3(2), April-June, 2012, pp. 36-49.

[4] Alafeef, M., Singh, D., Ahmad, K., Abu-Shanab, E. (2013).Usability Testing for Mobile Banking Prototype in Jordan.*Proceedings of the 2nd International Conference on Computer Engineering &Mathematical Sciences (ICCEMS 2013)*, 5-6 December 2013, Kuala Lumpur, Malaysia, pp. 48-54.

[5] Al-Sharafi, M., Arshah, R., Abu-Shanab, E., Fakhreldin, M. &Elayah, N. The Effect Of Security And Privacy Perceptions On Customers’ Trust To Accept Internet Banking Services: An Extension Of TAM. *COMSCET 2016*, Kuala Lumpur, Malaysia, 23-24 January, 2016, pp. 1-9.

[6] Archer, J. Boehme, A. Cullinane, D. PuhlmanN, N. Kurtz, P. and Reavis, J. (2012).Mobile Working Group Security Guidance for Critical Areas of Mobile Computing.Cloud Security Alliance, 2012.

[7] Bahar, A. Habib, A. and Islam, M. (2013).Security Architecture for Mobile Cloud Computing. International Journal of Scientific Knowledge, Vol. 3(3), PP, 11-17.

[8] Beach, A. Gartrell, M. &Han, R.L. (2009).Solutions to Security and Privacy Issues in Mobile Social Networking.In Computational Science and Engineering, 2009.CSE'09.International Conference on (Vol. 4, pp. 1036-1042). IEEE.

[9] Brandi, H.&Rosteck, T. (2004).Technology, Implementation and Application of the Trusted Computing Group Standard (TCG).Secure platforms provide new levels of security. Infineon White Paper.Datenschutz und Datensicherheit.Viewag.

[10] Caceres, R. &Sailer, R. (2006).Trusted Mobile Computing.In Proc. of IFIP Workshop on Security and Privacy in Mobile and Wireless Networks, Coimbra, Portugal.

[11] Chaturvedi, M. Malik, S. Aggarwal, P. and Bahl, S. (2013). Privacy & Security of Mobile Cloud Computing.Ansal University, Sector 55, Gurgaon-122011, India.

[12] Dagon, D. Martin, T. and Starner, T. (2004). Mobile Phones as Computing Devices: The Viruses are Coming! Pervasive Computing, IEEE, Vol. 3(4), PP, 11-15.

[13] Dinh, H. Lee, C. Niyato, D. & Wang, P. (2011). A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches .Journal of Wireless Communications and Mobile Computing, Vol. 13(18), PP, 1587-1611.

[14] Duckham, M. &Kulik, L. (2006).Location Privacy and Location-Aware Computing.Investigation in Change and Time.Dynamic & mobile GIS: investigating change in space and time, Vol. 3(1), PP, 35-51.

[15] Gligor, V. & Wing, J. (2011).Towards a Theory of Trust in Networks of Humans and Computers. In Security Protocols XIX (pp. 223-242).Springer Berlin Heidelberg.

[16] Josang, A. (2013). Identity Management and Trusted Interaction in Internet and Mobile Computing. IET Information Security, Vol. 8(2), PP, 67-79.

[17] Kaasinen, E. (2005). User acceptance of mobile services– value, ease of use, trust and ease of adoption. Behavior and Information Technology, Vol. 24(1), PP, 37-49.

[18] Kagal, L. Finin, T. & Joshi, A. (2001). Moving from Security to Distributed Trust in Ubiquitous Computing Environments, IEEE Computer, Vol. 34(12), PP, 154-157.

[19] Kagal, L. Undercoffer, J. Perich, F. Joshi, A. &Finin, T. (2002).A Security Architecture Based on Trust Management for Pervasive Computing Systems.Maryland Univ Baltimore Dept of Computer Science and Electrical Engineering.

[20] Khasawneh, R., Rabayah, W. & Abu-Shanab, E. (2013). E-Government Acceptance Factors: Trust And Risk. *The 6th International Conference on Information Technology (ICIT 2013)*, 8-10 May, 2013, Amman, Jordan, pp.1-8.

[21] Khiabani, H. Sidek, Z. and Manan, J. (2009). A Study of Trust and Privacy Models in Pervasive Computing Approach to Trusted Computing Platforms. In proceedings of the International Conference for Technical Postgraduates (TECHPOS '09), PP, 1–5, Kuala Lumpur, Malaysia, December 2009.

[22] Ko, S. Lee, J. and Kim, S. (2012). Mobile Cloud Computing Security Considerations. Journal of Security Engineering, Vol. 9(2), PP, 143-150.

[23] Kovachev, D. Cao, Y. and Klamma, R. (2010). Mobile Cloud Computing: A Comparison of Application Models. Journal of Arxiv preprint arXiv: 1107.4940.

[24] Kumar, S. (2004).Mobile communications: global trends in the 21st century. International Journal of Mobile Communications, Vol. 2(1), PP, 67-86.

[25] Laurila, J. Perez, G. Aad, I. Blom, O. Do, T. Dousse, O. Eberle, J. &Miettinen, M. (2012). The Mobile Data Challenge: Big Data for Mobile Computing Research. In Pervasive Computing (No.EPFL-CONF-192489).

[26] Lyle, J and Martin, A. (2010). Trusted Computing and Provenance: Better Together. In TaPP'10: Proceedings of the second USENIX Workshop on Theory and Practice of Provenance. 2010: San Jose, CA, USA.

[27] Mal-Sarkar, T &Bhunia, S. (2010). Collaborative Trust: A Novel Paradigm of Trusted Mobile Computing. arXiv preprint arXiv:1010.2447.

[28] Mavridis, I. and Pangalos, G. (2002).Security Issues in a Mobile Computing Paradigm.

[29] Nixon, P. Wagella, W. English, C. and Terzis, S. (2004). Security, Privacy and Trust Issues in Smart Environments: Technology, Protocols and Applications. Wiley, London, UK, pp. 220-240. ISBN 978-0-471-54448-7

[30] Poppa, D. Boudaoud, K. CremenE, M. and Borda, M. (2013).Overview on Mobile Cloud Computing Security Issues.RoEduNet 11th International Conference: Networking in Education and Research, Sinaia, Romania, January 17- 19, 2013.

[31] Ro, W. (2012).Report of Basic Principles for Increasing Security in a Mobile Computing Program. HTC Media Relations, htcpr@waggeneredstrom.com

[32] Robb, C. (2009). Security at the Edge — Protecting Mobile Computing Devices. NASCIO: Representing Chief Information Officers of the States.

[33] Sanaei, Z. Abolfazli, S. Gani, A. &Khokhar, R. (2012).Tripod of Requirements in Horizontal Heterogeneous Mobile Cloud Computing.arXiv preprint arXiv:1205.3247.I*nternational Conference on Computing, Information Systems and Communications.*

[34] Santos, N. (2013). Improving Trust in Cloud, Enterprise, and Mobile Computing Platforms, (Doctoral dissertation, Saarbrücken, Universität des Saarlandes, Diss., 2013).

[35] Satyanarayanan, M. Bahl, P. Caceres, R. and Davies, N. (2009).The Case for VM-Based Cloudlets in Mobile Computing.Pervasive Computing, IEEE, Vol. 8(4), PP, 14-23.

[36] Seigneur, J. (2005).Trust, Security and Privacy in Global Computing.Trinity College Dublin PhD thesis, technical report TCD-CS-2006-02. Retrieved from https://www.cs.tcd.ie/publications/tech-reports/reports.06/TCD-CS-2006-02.pdf

[37] Sinjilawi, Y., AL-Nabhan, M. & Abu-Shanab, E. (2014). Addressing Security and Privacy Issues in Cloud Computing. Journal of Emerging Technologies in Web Intelligence, Vol. 6(2), May 2014, pp. 192-199.

[38] Surie, A, Perrig, A. Satyanarayanan, M. and Farber, D. (2007).Rapid Trust Establishment for Pervasive Personal Computing. IEEE Pervasive Computing, Vol. 6(4), PP, 24-30.

[39] Surie, A. (2007). Improving Mobile Infrastructure for Pervasive Personal Computing (No.CMU-CS-07-163).Carnegie-

mellonunivpittsburgh pa school of computer science.

[40] Syme,R. (2009). Privacy of a mobile phone user in a rapidly evolving technological framework. Research Report, School of Mathematical and Geospatial Sciences, RMIT University.

[41] Valacich, J. (2003). Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments.Presented at Workshop on Ubiquitous Computing Environments, Washington State University.

[42] Winslett, M. Yu, T. Seamons, K. Hess, A. Jacobson, J. Jarvis, R. Smith, B. and Yu, L. (2001). Negotiating Trust on the Web.In: IEEE Internet Computing, Vol. 6(6), PP, 30-37.

[43] Wu, X, (2013).Research on Light-weight Trust Management Approach in Mobile Computing Environments. Journal of Communications, Vol. 8(12), PP, 877-882.

[44] Yan, A., Md-Nor, K., Abu-Shanab, E. &Sutanonpaiboon, J. (2009).Factors that Affect Mobile Telephone Users to Use Mobile Payment Solution, Int. Journal of Economics and Management, Vol. 3(1), pp. 37-49.

[45] Yan, Z. (2007). Trust Management for Mobile Computing Platforms. (Doctoral dissertation).Helsinki Univ.Of Technology, Helsinki, Finland.

[46] Zhang, C. Seifert, J. and Zhong, H. (2009). Secure Mobile Payment via Trusted Computing.In Proceedings of APTC 08 of third Asia-Pacific Trusted Infrastructure Technologies Conference, PP, 98-100.