QUALITY ASSURANCE ANALYSIS AND ENHANCEMENT ACTIVITY OF THE MANAGEMENT INFORMATION SYSTEM (MIS)

RUBINA ARSHAD*

AHSAN RAZA SATTAR **

FAHAD JAN***

Abstract

Software Engineering is a branch of computer science with new advancements and variety of software developed in different domains. In time, software systems become very large and complex due to repeated modifications and updates, needed to meet the ever changing requirements of the business. Therefore, information is the key force which drives businesses these days. To take timely and effective decision one needs correct and timely information. To build effective and efficient information systems, information is essential. Management information systems (MIS) are key expert-systems, which are designed to enhance the quality of production. This research was dealing with the amendments of the main architecture of the management information system (MIS) as well as to apply the standards like DSSs management standards. This effort is the first and foremost of its nature. Time complexity and space complexity are the major issues need to be addressed in the expert-system either for enterprise or for business purposes; hence these areas will be covered in this effort. Main focus of the research will be product an enhancement in accuracy, preciseness, efficiency and productivity rate of management information system (MIS).

Key Words: Management Information System, Decision Support System, Digital Signature Algorithm, Digital Signature Standards.

* Department of Computer Science, University of Agriculture, Faisalabad-38040, Pakistan

** Department of Computer Science, University of Agriculture, Faisalabad-38040, Pakistan

*** Department of Computer Science, University of Agriculture, Faisalabad-38040, Pakistan

Introduction:

Management information systems (MIS) are combination of computer hardware and computer software. These are used to process huge data to get required information. Many organizations prefer to use MIS systems to allow anyone to retrieve and change information easily and quickly. An MIS provides managers with information and support for effective decision-making, and provides feedback on daily operations. Outputs, or reports, are usually generated through accumulation of transaction processing data (Laudon and Laudon, 2009). Each MIS is an integrated collection of sub-systems, which are typically organized along functional lines within an organization. Management information systems were firstly designed to manage the information of the organization at a superior level (Cani, 1986). These systems were normally the subset of different working systems; however, these can also help improve the already existing system. MIS could be the part of an enterprise-system, education-system, business-management etc (Chen *et al.*, 1996). Now with the enhancement of the technology, the MIS are going to be used in decision-support systems or expert-systems.

A management information system (MIS) is generally thought of as an integrated system providing information to support operations, management and decision-making functions in an organization (Chih-Yuang *et al.*, 1999).The increasing interest in MIS had led to much activity in developing techniques and software for data management. MIS is basically concerned with the process of collecting, process, storing and transmitting relevant information to support the management operations in any organizations (Gennaro *et al.*, 1997). Management information system can be easily programmed by the owner to conduct certain actions at certain times (Friedman, 1993). In effect, managers can program the system to perform certain routines checks which can help in improving efficiency of a company through easy discovery of bugs or problems.

Furthermore, the programmability of most MIS saves a lot of priceless time and resources for owners. In other words, through programmability, business managers can program the system, to automatically discover certain deficiencies and even solve them (Dittmann *et al.*, 1998). There are two basic rules of this type, namely monitoring and evaluation which are "Fit for purpose", and "Right first time" (Blum and Paar, 2001). These services are basic used to maximize the probability. The minimum standards of quality are being attained by production process. The quality is being determined by the various users of the system. It is basically satisfaction of the user dynamically increasing demands. Different methods will be applied in the current research to fulfill different criterions of quality standards.

Materials and Methods:

Computers are important for more quantitative, than qualitative, data collection, storage and retrieval; Special features are speed and accuracy, and storage of large amount of data (Eoghan, 2011). MIS provides several benefits to the business organization: the means of effective and efficient coordination between Departments; quick and reliable referencing; access to relevant data and documents; use of less labour; improvement in organizational and departmental techniques; management of day-to-day activities (as accounts, stock control, payroll, etc.); day-to-day assistance in a Department and closer contact with the rest of the world (Turban and Jay, 2003).

The system under consideration with improved efficiency, accuracy and reliability will be developed with proper requirement engineering. The methods demonstrate the needs of the business environment. To improve a system because of two basic reasons; first, as the user work in a dynamic environment, the demands of the user change with the time line, and second reason is to lower down the space complexity.

To remove this time and space complexity of the current system one's needs to determine the requirements of that already build system. The research under consideration will perform in the number of steps as listed:

1. **Enhanced Architecture:** MIS architecture will be enhanced by the keen analysis of previous architectures and available MIS systems.
2. **Quality Indemnity Analysis:** Quality indemnity analysis will be performed by applying different standards to improve the efficiency of the current system.

Implementation of Digital Signature Algorithm:

With an addition to modules of decision support system, the current research focuses on the implementation of Digital Signature Algorithm (DSA). This algorithm was applied in the proxy agents of DSS. These agents were basically involved in the interlayer communication. During communication of different modules (as listed above) different data packets lost. So there was a need of certain standards, which was accomplished by the use of Digital Signature Algorithm (Bearman and Trant, 1998; Shih-Fu and Schneider, 1996).

This algorithm is used as a way of authentication of an electronic and digital document (text file, spreadsheet, e-mail, etc). Authentication is basically the whole detail about the particular message like who created the massage, when created the massage, why created the massage, till when it was last accessed, when it was edited etc (Storck, 1996; Hai-peng *et al.*,2009). This authentication process is basically dependent on certain types of encryption, where one can define encryption as a process of information transfer. This information transfer occurs between different modules of the management information system during the execution of query. As user send the particular query to the system, the data get transferred from one module to another. This transfer of data packets between different modules are basically encoded and decoded by the other module. In the authentication by the digital signature algorithm verification was performed, we applied a check that the resource of information is valid or not (Lin and Shih-Fu, 1999; Ying-Yu and Chong, 2008). So, as a result two process move side by side to each other that includes encryption and verification.

Steps of Implemented Digital Signature Algorithm:

Digital signature algorithm is named because of its property to add up signature to a particular massage. Signature is basically defined as the unique identification key.The digital signature algorithm was implemented in the proxy agents by following a number of steps which move recursively to complete the process of data hiding as well as data verification.

The digital signature whole scheme is divided into two parts as Signature Generation and Signature Verification.

The two boxes separately describe the signature generation and signature verification. These are actually the two separate systems over the internet that performs the act of massage transfer. One system which transfers the massage has the private key while the other one have the public key. The massage along with its key is send to digital signature algorithm in both cases. In sender system the signature verification occurs while in the receiver system digital signature algorithm perform the function of signature verification.

The start of this algorithm a random number get picked on which we have applied different mathematical operations and compute the value of r as well as s. (r, s) are the parameters of digital signature. These values corresponds to the value of m i.e. massage (send by a system or a module during the communication of agents within a system). This massage m is considered as any amount of data and DSA concerns with the validation and verification of this data that at each and every stage of record transmission the values are saved in its original format. This is done to check that no other binary record or garbage stored values are incorporated within the original massage, hence making the transfer secure.

The value of r is computed first and sends to another algorithm known as Hash algorithm. This algorithm takes input of massage m. this algorithm take the massage and convert the massage into the 64 bit system code. This code is generated by the two alphabets combination each consisting of 32 bit massage.

After exit from the hash algorithm system generates the s value. These values along with the massage are than sent to the receiver end. The receiver takes the massage m and its signature r and s and decodes the massage again. This value is actually the recovery of the massage in the form of gk MOD p. The recovery verification has a check point that the massage is original or having other value. If the value of massage will be the same algorithm verifies it otherwise rejection is done by the receiver module.

Implementation of Digital Signature Standards:

The Digital Signature Standard (DSS) is the format which is used for the digital signatures. This format was endorsed by the US government. This was applied in the current research, which was based on a type of public key encryption method. This encryption method was utilized in the

Digital Signature Algorithm (DSA). These standards were followed to save the record and avoiding unneeded information which spoils the original massage.

Results and discussion

Current research was the enhancement of the already defined system for human resource management. The current system was modified with high efficiency and accuracy by adjoining of the system with the decision support system. Decision support system is the system, which have the ability to work intelligently and cope the changing environment.

Incorporation of Decision Support System in Management Information system

The development of new and enhanced management information system architecture and its environments requires new concepts of both the support to the new working process and to protect the multimedia data during the production and distribution. This architecture addresses authentication and copyright protection as major security demands in digital management information system. Management information system is devided into three functional modules now it consists of following parts which are Dialogue Management System (DGMS), Data Base Management System (DBMS), Model Based Management System (MBMS). The enhanced architecture is given in the figure below (Figure 3.1).

Dialogue Management System (DGMS)

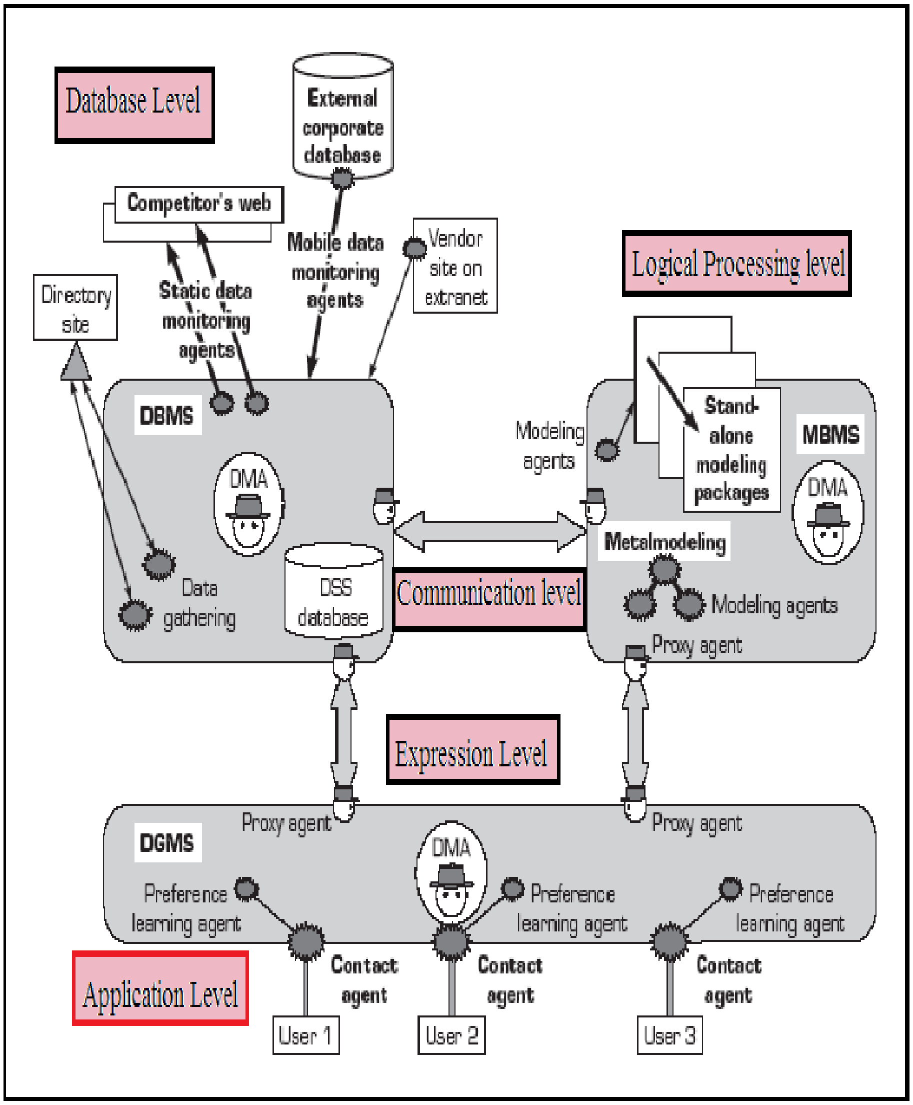
Three types of agents are involving in DGMS **Contact Agents:** Users interact DGMS with the help of these agents. **Preference Learning Agents:** These agents identify the preferences of the user. **Proxy agents:** These agents control the provide between different parts of the system.

Data Base Management System (DBMS)

The following agents are involved in DBMS **Mobile Data Monitoring Agents:** These agents extract data from external corporate database. **Static Data Monitoring Agents:** These agents monitor competitor's web sites **Proxy Agents:** These agents provide the communication between DBMS, DGMS and MBMS. **Data Gathering Agents:** These agents provide data to Directory Site. Some other agents also involved that extract data from Vendor site

Model Based Management System (MBMS)

The following agents are involved in MBMS: **Modeling Agents:** These Agents create the model of the data. **Proxy Agents:** These agents provide the communication between DBMS, DGMS and MBMS. **Meta Modeling Agents:** These agents create Meta data



Enhanced Architecture of Managemenet Information System with an intergration of Decision Support System

Figure 4.1: Enhanced MIS Architecture

Levels of Current MIS:

Except these separate systems we have defined different levels of the architecture. This procedure was performed to make the hierarchy of the system. These levels are Application level, Expression level, Logical processing level, Communication level and Database level.

Application Level

Application level includes the client information, which deals with the multiple users and cope up with their quires. This layer processes the user quires and generates results on the basis of all the available records. It is the first and foremost phase of application server for the handling of request to the Web Action.

These actions are based on the different requests sanded by users, which are named as firstly downloaded and cached from the configuration files and the database. As the query executed it will active certain Web Action. The front-end controller will dynamically load the Web Action. This layer is the same as it was previously implemented. The only enhancement in the system is the introduction of multi user access to the system at a single moment of time. The access was previously provided by the static entities but now the intelligent agents are used in this level, which are known as contact agents.

Expression Level

Second level of architecture multi-layer system is the expression level, this level utilizes the agents known as preference learning agents. These agents have the ability to learn from the system.

Logical Processing Level

Logic layer interaction is done with the data persistence layer, in which business logic layer provides the interface and the data persistence layer provides the implementation. When the implementation framework of the data persistence layer is changed, the work of the business logic layer will not be affected, thus the system flexibility and maintainability is maintained. The logics of the system are now saved in the form of models these models are based on the dimensionality of the records. The agents that are utilized for this type of modeling are known as modeling agent. Which intelligently pick the record from various DBMS sources systems and model the record according to their connections and linkage.

Communication Level

Communication layer have the main responsibility of communication, it communicates between the logical processing layer and the database layer. In the current architecture this procedure is performed by the agents known as proxy agents.

Database Level

Database layer is the data repository which manages all the records of an organization, which are required by the user at a particular time against a particular query. The enhanced level provides different intelligent agents to cope with the problem of data handling from different systems. These agents include Static data monitoring agents, Dynamic data monitoring agents, Data generating agents. Static data monitoring agents get the records from the defined directories and databases available to the system. Dynamic data monitoring agents have the capability to get the record from dynamically changing environment.

Implementing Digital Signature Algorithm (DSA):

In the current research the architecture of the system was enhanced by applying the Digital signature algorithm. This algorithm was initially used in the hardware systems to reduce the package loss. Now in the current approach this algorithm is utilized in collaboration with the artificially intelligent agents.

This method was used to provide a way for the generation as well as verification of digital signals. The requirements of the method were the pair of public and secret keys as well as values. These values are selected according to the rules of the algorithm applied. In the current system implementation of the digital signature scheme is used for the efficient and active usage in any level of the architecture. This architecture is based on various levels as well as various active agents contributing in each subsystem of the architecture. The implementation of the current algorithm reduces the package loss in the communication of different agents of the system.

Implementing Digital Signature Standards (DSS):

As the human resource management includes the record of digital signatures in databases so a Federal Information Processing Standards Publications in June 2009 announce the DIGITAL SIGNATURE STANDARD (DSS) were applied in the current research. This was done for the act of Computer Security. This Standard specifies algorithms for applications requiring a digital signature, rather than a written signature. A digital signature is represented in a computer as a string of bits. A digital signature is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data. Signature generation uses a private key to generate a digital signature; signature verification uses a public key that corresponds to, but is not the same as, the private key. Each signatory possesses a private and public key pair. Public keys may be known by the public; private keys are kept secret. Anyone can verify the signature by employing the signatory's public key. Only the user that possesses the private key can perform signature generation.

References:

- Bearman, D. and J. Trant. 1998. Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process. D-Lib Magazine, 1(0): 39-48.
- Blum, T. and C. Paar. 2001. High–Radix Montgomery Modular Exponentiation on Reconfigurable Hardware. IEEE, 50(7):759-764.
- Cani, J. F. 1986. A computational approach to edge detection. IEEE Trans on Pattern analysis and Machine intelligence, 8(6):679-698.
- Chen, P., S. Hwang and C. Wu. 1996. A systolic RSA public key cryptosystem in Proceedings of International Symposium of Circuit and System. IEEE, 4(1):408-411.
- Chih-Yuang, S., S. Hwang., P. Chen and C. Wu. 1999. An Improved Montgomery's Algorithm for High-Speed RSA Public-Key Cryptosystem. IEEE, 7(2):280-284.
- Dittmann, J., S. Mark and S. Ralf. 1998. Robust MEG Video Watermarking Technologies, Proceedings of ACM Multimedia'98. The 6'h ACM International Multimedia Conference, Bristol, England, 7(1):71-80.

- Eoghan, C. 2011. The increasing need for automation and validation in digital forensics. Digital Investigation, 7(3):103-104.
- Friedman, G.L. 1993. The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image. IEEE Trans on Consumer Electronics, 39(4):905-910.
- Gennaro, R., H. Krawczyk and T. Rabin. 1997. RSA-based Undeniable Signatures. CRYPTO '97, Santa Barbara, CA, USA, 45(7):945-957.
- Hai-peng, C., S. Xuan-jing and W. Wei. 2009. Digital Signature Algorithm Based on Hash Round Function and Self-Certified Public Key System. IEEE, 2(0):618-624.
- Harn, L., M. Mehta and H. Wen-Jung. 2004. Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA). IEEE, 8(3):198-200.
- Laudon, K. and J. Laudon. 2009. Management Information Systems. Journal of computer science, 11(13):627-629.
- Lin, C. Y. and C. Shih-Fu. 1999. Issues and Solutions for Authenticating MPEG Video. SPIE Storage and Retrieval for Image and Video Databases, San Jose, CA, USA, 2(5):111-123.
- Shih-Fu, C. and M. Schneider. 1996. A Robust Content Based Digital Signature for Image Authentication. Digital Signal Processing, 20(5):270-230.
- Storck, D. 1996. A New Approach to Integrity of Digital Images Proceedings of IFIP World. Journal of computer science, 13(8):14-123.
- Ying-yu, C. and F. Chong. 2008. An Efficient Implementation of RSA Digital Signature Algorithm. IEEE, 2(0):100-103.