Security Approaches For Integrated Enterprise Systems Performance: A Review

Subhi R. M. Zeebaree, Rizgar R. Zebari, Karwan Jacksi, Dathar Abas Hasan

Abstract:— Advancement in Information and Communications Technology (ICT) have become the communication medium for virtually every small or large industry around the world. This technology changed the ways of doing businesses and has led to the invention of a new concept called Electronic Business (E-Business). E-Business involves various activities for any businesses such as ordering, transacting, customer servicing, delivering and paying. This new type of business consists of many advantages comparing with the traditional form of business, but on the other hand, it faces real challenges related to the approaches used to keep the data secure. The sharing of the sensitive data for any enterprise system requires designing a security management framework in order to enable controlling access to the sensitive information. In this paper, the last efforts of researchers proposed in security field of the E-Business systematically reviewed. Furthermore, the security approaches, techniques and security frameworks have been discussed.

Index Terms:— Enterprise Security, Authentication; Digital Signature; Encryption; Encryptions; E-Business; Enterprise Systems.

1 INTRODUCTION

NOWADAYS the dependency on Enterprise systems (ES) by almost organizations around the world is on a continuous increase. ES is a collection of applications that automate business processes and manages business data. The most important facilities of ES system are integrity and information system configuration that manages and plans the resources of the enterprise system. As well as incorporating and streamlining the business processes across and within the technical or functional boundaries in the system [1]. However, information is the most important asset for any corporations, it may contain information about agents' activities, sales reports, bank accounting …etc. The organizations and companies that deal with enterprise data have to be proactive by systematic approaches to manage and evaluate the online security of their services and to face any information security threats. E-business security is affected by computer security, data security, network security and it is a part of the information security framework [2]. The most important factor for protecting E-business accomplishments is to depend on a standard and systematic security practice and guidelines [3]. For the semantic web technology, the techniques are presented in [4]–[10]. ES information safety from the different types of threats is vital. Integration of organization's data and operation procedures can be attained by information security through working together of systems, operations, and internal controls. Extremely, the process of securing enterprise systems is difficult task, it requires techniques such as encryption, integrity and access control to be provided and installed on the computer systems. These techniques are a part of the solution; the other part is the need to construct security architecture for business environment including processes, policies, and technologies in order to provide a total security [11]. This Paper focuses on the most effective approaches for overcoming the security challenges and then evaluating of the overall security system is needed to measure the effectiveness of the security [12].

2 SECURITY APPROACHES FOR ENTERPRISE SYSTEMS

As information is the most important part of any organization depends on an enterprise system. Hence, numerous researchers focus on the information security issues and the ways by which the information can be safe and free of risks. Generally, for performing online business there are three basic security issues: how to verify the identity of the person we are doing business with, ensuring that any message received or sent will not be tampered with, the last issue is getting an evidence about the time, date, and place of signing the contract [13]. These three issues can be solved by the following techniques:

2.1 Authentication

The most important problem that researchers tried to solve in enterprise systems is an authentication of the partners. It is the mean by which each partner can prove himself to another and vice versa. Therefore, to consolidate an authentication mechanism various academics suggested a new technique. Oluwafemi et al. [14] thought that one-way authorization is not effective to secure enterprise data because hackers have the abilities to invent different manners to attack enterprise system. This unauthorized access acts as a security challenge and it is not enough to protect data. Therefore, they proposed a technique which enables both sides in a communication system to be authenticated for each other, it is called two-way mobile authentication as shown in Fig. 1.

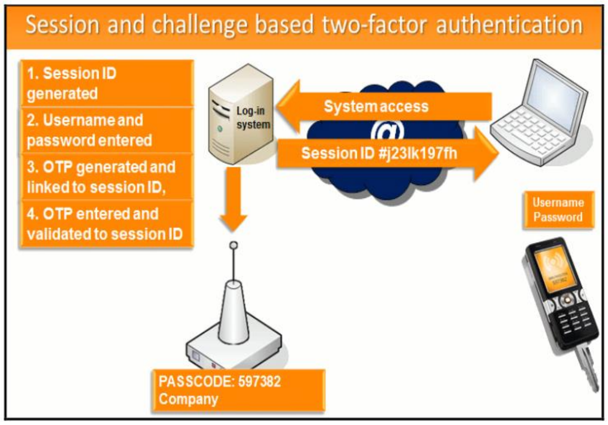
Session and challenge based two-factor authentication
1. Session ID generated
2. Username and password entered
3. OTP generated and linked to session ID,
4. OTP entered and validated to session ID
Log-in system
System access
@
Session ID #j23lk197fh
Username Password
PASSCODE: 597382 Company

***Fig. 1**. Two-way Mobile Architecture [4]*

By using personalized data information requirement, the system will be more effective for providing more secure authentication. The mechanism of Two-way mobile communication started when the user inputs his/her username and password to the system. Then if the user success to log in, the system will send SMS code to the user phone number. At that time the user will redirect this code back to the system, at this point user and enterprise system will be authenticating for each other. Wang et al. [15] believed that the use of fixed user IDs in enterprise system login module is not sufficient and possible to be cracked. Therefore, the system management and monitoring will be meaningless as a result of illegal access. However, the fingerprint identity may be the solution towards designing a security framework for an Enterprise system. Fingerprint products are widely used in ES because the required technologies developed and the equipment being manufactured on a large scale which causes a fast dropping in cost. The researchers in [13] depended on fingerprint authentication due to three factors. The first is personal information which consists of information about users such as ID, first name, last name, address, position, etc. The second is that all other authentication like a dynamic password card, mag card, USB key, IC card, and flash drive, can all be cracked and then misused except the living fingerprint. The third is that the fingerprint is a unique characteristic which can be employed to identify users and considered the safest factor because of duplicating the fingerprint is impossible.

2.2 Digital Signatures

Digital signatures defined as a mathematical scheme that can be used to verify the authenticity of a digital document or message. Digital signatures are usually used for software distribution, financial transactions, and in other cases where it is important to detect fake or damaging. When encrypted digital signature implementing is required, the digital signatures can be used as a means. This technology lets the receiver of a document to approve the source's individuality also it attends to show the validity of the received document has not been damaged with [16]. Saha et al. [17] designed a digital signature model based on asymmetric key cryptography concept. Both digital signature and manual signature confirms the document ownership. Moreover, for confirming that the document has been created by the owner and it is not changed in transportation, a valid digital signature was used. Signing and verification are two main processes were executed to create digital signature application. In signing process, hash value has been calculated by applying cryptographic hash function at the sender's side date. Hence, they used signer's private key in order to produce the signature. Also, for obtaining a document that is digitally signed, the third-party issues certificate along with the signature was attached to the data. The hash function has been executed on the data at the receiver end and hash value generated for starting the verification process with checking the signature. The signer's public key used for performing decryption process encrypted signature generating another hash value. The signature validity depended on the equality of both two hash values. Mathew and Saranya [18] developed a system has the ability to use the biological property to generate digital signature. They utilized mobile devices of users which consist of built-in fingerprint sensor as well as the front camera. The process starts with inputting username and password then using front camera to capture a personal picture of the user. The last step was using the fingerprint sensor to record the fingerprint. After executing the above steps, a digital signature of the fingerprint was created and embedded in the image of the face in order to generate a pictographic password. The final step was to send this pictographic password to the database for verification. Verification of the user authenticity procedures starts with checking the username and password. Afterward recognizing face to assure that the face stored is the same as that captured. Later, the digital signature will be read to verify that the image hasn't been changed during the transmission process. Finally, for further authentication, the fingerprint itself will be checked. Passing all these steps successfully will allow complete authentication, otherwise, the user will be access denied. This security system doesn't require any additional hardware equipment; it uses only built-in hardware in the mobile device. The use of pictographic password will cause user access denied if any individuals try to tamper the digital signature.

2.3 Encryption

It is a part of cryptography, which involves converting message information into a code which is not readable. The encrypted message information will be decrypted at the receiver side in order to be usable and understandable. Hence key is used to identify the data to a certain individual or organization. In public key encryption two keys are used one is private and the other is public. The first one is used for encryption procedure and the second key for decryption process [19]. Harfoushi et al. [20] Suggested that a better solution for securing information is Encryption. Permissions were given by data owners to some particular group elements to access data easily. A security heterogeneous data-centric was employed in order to provide data access control. A security model of data was consisting of authentication, data encryption, and data integrity. The data to be secure efficiently in the cloud, users' data recovery protection has to be designed. Moreover, for ensuring the security and privacy of data the protection service of data can be used. To prevent data to be accessed by others, data will be encrypted totally and it will unusable. When users wish to upload data into cloud servers [21], [22], they should be sure about that data is saved on backup drives. Also calculating the hash file is needed in order to be sure that data will not be altered. Panwar et al. [23] Proposed a system for sharing patient information based on the QR code, the used technique involved QR code of encrypted private message which was encoded with C#.NET. The first step of the encryption process was entering personal information of the patient, and then dividing this information into the blocks of 64-bit. Afterwards the blocks encrypted using DES algorithm, finally saving the ciphertext. Generating QR code take place through executing C#.NET program on encrypted message, the output encoded message was sent to the receiver for recovering the secret message via decryption process. On the side of receiver, the message received through secure communication channel then the QR code generated for decoding the image by the shared program. By scanning application code, the encrypted ciphertext from QR code extracted, DES algorithm applied to the blocks which led to getting the patient information safely.

2.4 Cloud Based Security Framework for Enterprise Systems

Binu and Meenakumari [1] proposed a security framework based on the cloud for enterprise systems. The suggested system was consisted of five modules and each system module had its own task to perform as shown in Fig. 2.

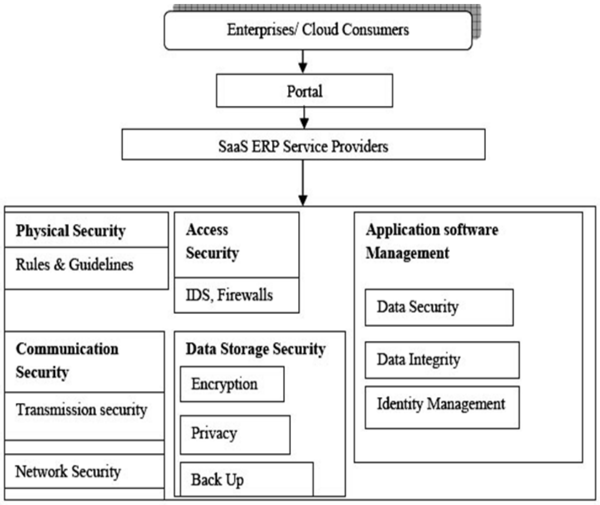

***Fig. 2**. Security framework for enterprise systems based on cloud*

Defining and enforcing the rules of conduct was performed by physical security management module. As well as the system was included of mechanisms for ensuring that rules were executed. Data storage security Management Module enabled sensitive data to be encrypted as it was stored in cloud database system [24], [25]. The last task of the module was performing data backup for user's data in order to be recovered in urgent case. Moreover, for securing the system against Denial of Service (DoS) attack there was intrusion detection mechanism in the access security management module. Another module which was application software management consisted of business logic to ensure the integrity and security of data. As well as the above module included mechanisms for user authentication for providing service. The identity management task was performed by business logic. The security of information which was communicated inside cloud environment was guaranteed by communication management module (the last module of the system).

2.5 Logical Security Framework for E-Commerce System Based on Service Oriented Architecture (SOA)

Luhach. et al. [26] designed a security system based on SOA for e-commerce which called logical security framework and depended. The security framework system was involved of two behaviors (land access and remote access). The business service component to be available to clients and to validate a proper authentication, two-tier security was preserved on the web server [27],[28]. Therefore, generating a duplicate certificate or forging the certificate have been prevented from the user. The proposed security system executed as follows: the user's data are sanitized firstly then forwarded to the server according to sanitization rules then user demanded to access the server through HTTP protocol. Hence, this step prevented the user attempt to bypass the authentication and solving the risks of certificate duplicity. Apache mod-security was used as a second layer of the designed security system. If the first layer (sanitization layer) was avoided, the next security layer which is rule-based plug-in could block the attempt. Henceforth, malicious requests were to the business service components were denied by the rules created on the system.

3 Security Evaluation and Analysis for Enterprise Data System

Designing an effective security system for enterprise system depends on many factors; one of a most important factors is the security system evaluation. Evaluating of the security system should involve all parts of the system [29]. Alshammari [30] evaluated the architecture of the security system which was an important concept to identify overall security of any program. Various security models have been suggested by researchers to evaluate security systems and they designed a security evaluation model for enterprise system. Despite that the security system dialed with three-tier architecture model there was an extra level. There were a number of metrics for each level of the security levels for the proposed system security at a certain abstraction level. In the three layers, many structural properties metrics related with the security work with each part in each layer had a direct impact on them in terms of the potential flow of classified data. Additionally, the total security of the entire enterprise system was summarized with the top level which provided a single security measurement.

This led to easily comparing the proposed system with other similar systems. Shrivastava et al.[31] Presented a novel technique and they proposed algorithms for model numerous aspects of system dependencies and performing impact analysis respectively. The system components and their inter-relationships in the form of an influence graph were demonstrated by the technique. This step was considered as first key idea solution of the system and based on weighted directed acyclic graph (DAG). While the proposed algorithm represented as second key of the system solution was derived the system health in the event of a change. The impact propagation algorithm was based from traverses of the influence graph through various weighted edges and the dependency metaphors to derive the impact analysis. Wang et al. [32] Proposed a system for the e-commerce website to test and evaluate the security vulnerabilities. The designed system was entailed of security testing module and the result evaluation module as shown in Fig. 3. Moreover, the system was designed to tackle various security attacks such as SQL injection attack which could be used to get critical information from the database.

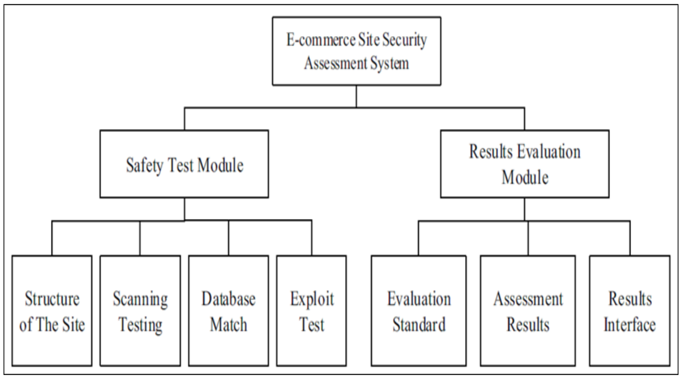

***Fig. 3**. Architecture of E-Commerce Site Security Evaluation System [13]*

The test module was run by a penetration test. Vulnerability scanning technology was the start of the process which was used to test the security of all aspects of the network. The obtained results from the safety evaluation module perform a test on test module results. The assessment of the proposed security system involved the security testing module and result evaluation module.

4 Discussion

The main aim of this paper is to study many techniques that proposed to build an effective security system for enterprise systems. These techniques include verification, monitoring, and evaluation of different activities in an enterprise system. The authenticating process is updated because the classical login may not be secure enough due to the penetration risks by hackers. Furthermore, using the biological properties such as fingerprints and face recognition of an individual in authentication may be more secure compared to traditional methods. Also, these biological properties have many benefits in designing a digital signature system. Encryption of sensitive data may be the best solution to keep it secure; this data can be encrypted using a special algorithm before storing it in the cloud. The backup process can be used in periodically to keep a copy of users' data away from accessing by hackers and recovering it when we need it. The table 1 shows main differences between the techniques discussed in this paper.

TABLE 1

Techniques Used in Enterprise System Security

Reference	*Authentication*	*Digital Signature*	*Encryption*
Ayangbekun Oluwafemi J. et al. [12]	*Two-way Authentication using Mobile SMS code*	-	-
FengWang et al. [13]	*Using fingerprint to generate login system*		
Goutam Saha. et al. [14]	-	*using hash value to generate a digital signature*	-
Sherly Mathew et al. [15]	-	*Composition of fingerprint and face pic is used to build a digital signature*	-
R. Velumadhava Rao. et al. [16]	-	-	*Encoding data before storing on cloud as well as enabling data recovery*
Narendra Panwar et al. [17]	-	-	*Encoding QR code of encrypted message with C#.net app.*

5 Conclusions

An enterprise system involves packaged software that automates, increases the performance of business processes and manages business information. The information is valuable for the organization and usually is a targeted by the different types of attack. In order to visualize the risks and how protecting data against them. Therefore, in this paper we presented and reviewed a numerous of security approaches such authentication, digital signature and encryption as well as other proposed frameworks. The evaluation of the security system is a very important factor to develop the overall security; therefore, we focus on some methods of security system evaluation.

References

[1] M. S. Binu and J. Meenakumari, “A security framework for an enterprise system on cloud,” Indian Journal of Computer Science and Engineering (IJCSE), vol. 3, no. 4, pp. 548–552, 2012.

[2] M. Niranjanamurthy and D. Chahar, “The study of e-commerce security issues and solutions,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 7, pp. 2885–2895, 2013.

[3] R. R. Zebari, S. R. Zeebaree, K. Jacksi, and H. M. Shukur, “E-Business Requirements For Flexibility And Implementation Enterprise System: A Review.”

[4] K. Jacksi, “Design and Implementation of E-Campus Ontology with a Hybrid Software Engineering Methodology.”

[5] A. AL-Zebari, S. R. M. Zeebaree, K. Jacksi, and A. Selamat, “ELMS–DPU Ontology Visualization with Protégé VOWL and Web VOWL,” Journal of Advanced Research in Dynamic and Control Systems, vol. Volume 11, no. 01-Special Issue, pp. 478–485, 2019.

[6] R. Ibrahim, S. Zeebaree, and K. Jacksi, “Survey on Semantic Similarity Based on Document Clustering,” Adv. Sci. Technol. Eng. Syst. J., vol. 4, no. 5, pp. 115–122, 2019.

[7] K. Jacksi, N. Dimililer, and S. R. M. Zeebaree, “A Survey of Exploratory Search Systems Based on LOD Resources,” in PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON COMPUTING & INFORMATICS, COLL ARTS & SCI, INFOR TECHNOL BLDG, SINTOK, KEDAH 06010, MALAYSIA, 2015, pp. 501–509.

[8] A. Hasso, K. Jacksi, and K. Smith, “Effect of Quantization Error and SQNR on the ADC Using Truncating Method to the Nearest Integer Bit,” presented at the 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019, pp. 112–117.

[9] K. Jacksi, N. Dimililer, and S. R. Zeebaree, “State of the Art Exploration Systems for Linked Data: A Review,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 7, no. 11, pp. 155–164, 2016.

[10] S. R. Zeebaree, A.-Z. Adel, K. Jacksi, and A. Selamat, “Designing an ontology of E-learning system for duhok polytechnic university using protégé OWL tool,” Journal of Advanced Research in Dynamic and Control Systems, vol. 11, no. 05-Special Issue, pp. 24–37, 2019.

[11] J. Alqatawna, “The Challenge of Implementing

Information Security Standards in Small and Medium e-Business Enterprises," Journal of Software Engineering and Applications, vol. 7, no. 10, p. 883, 2014.

[12] M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things Security: A Survey," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 162–166.

[13] F. Meskaran, Z. Ismail, and B. Shanmugam, "Online purchase intention: Effects of trust and security perception," Australian journal of basic and applied sciences, vol. 7, no. 6, pp. 307–315, 2013.

[14] A. Oluwafemi J., O. Sunday, and O. Shoewu, "Two Way Mobile Authentication Security Mechanisms for an Enterprise System," Oct. 2014.

[15] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li, "A system framework of security management in enterprise systems," Systems Research and Behavioral Science, vol. 30, no. 3, pp. 287–299, 2013.

[16] R. Patel, "IMPORTANCE AND IMPLEMENTATION OF DIGITAL SIGNATURE IN OFFICE DOCUMENTS," Oct. 2019.

[17] G. Saha, M. Desai, A. Ghosh, and N. Saha, "Digital Signature Modeling in E-Business," in 2014 IEEE 11th International Conference on e-Business Engineering, 2014, pp. 350–354.

[18] S. Mathew and G. Saranya, "Advanced biometric home security system using digital signature and DNA cryptography," in 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), 2017, pp. 1–4.

[19] T. Virtue and J. Rainey, "Chapter 4 - Privacy and Security in Healthcare," in HCISPP Study Guide, T. Virtue and J. Rainey, Eds. Boston: Syngress, 2015, pp. 61–89.

[20] O. Harfoushi, B. Alfawwaz, N. A. Ghatasheh, R. Obiedat, M. Mua'ad, and H. Faris, "Data security issues and challenges in cloud computing: a conceptual analysis and review," communications and Network, vol. 6, no. 01, p. 15, 2014.

[21] Z. N. Rashid, S. R. M. Zebari, K. H. Sharif, and K. Jacksi, "Distributed Cloud Computing and Distributed Parallel Computing: A Review," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 167–172.

[22] K. Jacksi and S. M. Abass, "Development History Of The World Wide Web," vol. 8, no. 09, p. 6, 2019.

[23] N. Panwar, M. S. Rauthan, and A. Agarwal, "Privacy of Patient Information: Implementation and Security Analysis of a Secure Three Tier Patient Information System Based on QR Code," in 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2016, pp. 232–234.

[24] K. Jacksi, "Design and Implementation of Online Submission And Peer Review System: A Case Study Of E-Journal Of University Of Zakho," Int J Sci Technol Res, vol. 4, no. 8, pp. 83–5, 2015.

[25] K. Jacksi, F. Ibrahim, and S. Ali, "Student Attendance Management System," Scholars Journal of Engineering and Technology (SJET), vol. 6, no. 2, pp. 49–53, 2018.

[26] A. K. Luhach, S. K. Dwivedi, and C. K. Jha, "Desiging a logical security framework for e-commerce system based on soa," arXiv preprint arXiv:1407.2423, 2014.

[27] K. Jacksi, S. R. Zeebaree, and N. Dimililer, "LOD Explorer: Presenting the Web of Data," Intl. Journal of Advanced Computer Science and Applications, vol. 9, no. 1, pp. 45–51, 2018.

[28] R. R. Zebari, S. R. Zeebaree, and K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 156–161.

[29] W. J. Brooks, M. J. Warren, and W. Hutchinson, "A security evaluation criteria," Logistics Information Management, vol. 15, no. 5/6, pp. 377–384, Jan. 2002.

[30] B. M. Alshammari, "An Assessment Model for Security-Critical Enterprise Systems," International Journal of Information and Education Technology, vol. 4, no. 4, p. 323, 2014.

[31] M. Shrivastava, M. Natu, and V. Sadaphal, "Towards predictable and risk-free enterprise systems," in 2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA), 2015, pp. 1–7.

[32] X. Wang, K. Zhang, and Q. Wu, "A Design of Security Assessment System for E-Commerce Website," in 2015 8th International Symposium on Computational Intelligence and Design (ISCID), 2015, vol. 1, pp. 137–140.