DOI: 10.24996/ijs.2021.62.2.30

ISSN: 0067-2904

Design and Implementation of an IoT-based Transactional System for Quality Management

Mohammed Issam Younis*, Athraa H. Alwan

Computer Engineering Department, College of Engineering, University of Baghdad

Received: 31/3/2020 Accepted: 14/7/2020

Abstract

The spread of Coronavirus has forced populations around the globe to adopt strict measures such as lockdown, home quarantine, and home office. Moreover, in the current development of network communications, people can exploit internet and intranet features in many systems that need to be faster, more efficient, and available on time. Furthermore, with the benefits of using internet-of-things (IoT), through which things are generated, gained, discovered, and proposed without interference, the user could receive the last status without exertion and direct contact (i.e., in a contactless manner). These specifications can be used in a transaction system. This paper proposes an electronic transaction system (ETS) as a replacement for the current paper transaction used in most organizations' environments. The progress includes the signing privilege, access right for each position, delivery reports, transaction tracking, and transaction storage safety. Transactions will be stored in an encrypted way at the database to keep them safe from illegal changes. For that, a secure electronic transaction is created with digital signature services. The negligence can be identified in the workflow by tracking the operations and receiving exceptional cases' alerts. Finally, this paper compared the proposed system against state-of-the-art systems.

Keywords: Digital signature, Database cryptography, Transaction system, IoT.

تصميم وتنفيذ نظام المعاملات القائم على إنترنت الأشياء لإدارة الجودة

محمد عصام يونس*، عذراء حسين علوان

قسم هندسة الحاسبات، كلية الهندسة، جامعة بغداد، بغداد، العراق

الخلاصة

مع الانتشار الحالي لفايروس كورونا اصبح لزاما البقاء في البيوت وتبني العمل الالكتروني عوضا عن الورقي لإنجاز المعاملات. نظراً للتطور الحاصل في الشبكات والاتصالات في الجامعات والمؤسسات اصبح من الامكان استغلال هذا التطور في عدة مجالات منها اقتراح نظام المعاملات الالكترونية عوضاً عن المعاملات الورقية المعتمدة في الجامعات مما يسهل عمليه تبادل المعلومات و سرعة النقل و سهولة التواصل بين كادر المؤسسة مما يجعل بيئة العمل سريعة و ملائمة واكثر كفاءة من التبادل اليدوي. علاوة على ذلك مع فوائد (انترنت الاشياء) عدة اشياء سوف تنشىء, تأخذ و يتم الكشف عنها و اقتراحها دون تدخل المستخدم مما يسهل عمليه التدقيق ومعالجة البيانات. ايضاً طريقة التوقيع الالكتروني توفر اتصال امن و موثوق في نظام المعاملات عندما يكون التوقيع صالح يمكن للمستخدم التأكد من ان المعاملة صادرة من جهة موثوقة و من

*Email: younismi@gmail.com

موظف ضمن المؤسسة, ايضا لا يمكن للمستخدم انكار اصدار معاملة كونها تحمل توقيعه الالكتروني. ايضا
يمكن استغلال التوقيع الالكتروني في متابعة المعاملة و معرفة سبب تأخرها و الموظف المقصر في سير
المعاملة. و لحفظ المعاملة من التغييرات الغير مسموح بها و حفظها من السرقة و معرفة البيانات يتم حفظ
المعاملة في قاعدة بيانات مشفرة. تستعرض هذه الورقة أنظمة المعاملات و التوقيع الأوتوماتيكي الحديثة
وتوضح مزايا وعيوب كل نهج من خلال توفير مقارنة قائمة مرجعية. بخلاف الأعمال السابقة ، فإن النظام
المقترح يحمي البيانات من الضياع ويضمن وصولها إلى المستخدمين بدون اي تغيير مع ضمان معرفة
مصدر المعاملة و فحص التواقيع المرفقة ضمن المعاملة.

Introduction

Electronic transactions have significantly evolved in recent years. Because of the significant developments in information technology, electronic transactions increased in size and use and expanded to a service provider’s form and promoted products. An electronic transaction is a form of integrated use of information and communications technologies. The purpose of this integrated form is to facilitate and accelerate multiple purchases, with a guarantee of high accuracy. Numerous applications are widespread in all government agencies, but they differ by the organization’s needs, such as billing systems and file-keeping systems, etc.

Many applications are vulnerable to steal, such as email, e-commerce systems, and e-banking systems. Therefore, data security is needed for the stored and transferred data [1]. The cryptosystem changes the data into a code sent through the network, making it unreadable without authorized keys [2]. Most organizations replace the paper environments with electronic environments, and word processing returns the transaction to handwriting. In contrast, manual spreadsheets are replaced by corresponding applications, with less use of paper and pen, where emails replace handwritten letters. The transformation from paper-intensive to the paper-free environment makes the organizations avoid traditional and paper operations that consume time; also, organizations improve efficiency by searching for a creator technology and becoming more practical. While internet services are widespread worldwide, and each organization has its servers and networks, organizations can exploit these resources to build such a system that can be a shared platform with the needed specifications. An intranet is similar to the internet, but it is designed for a specific group of users, which allows the organization to limit network access among particular users.

Kevin Ashton coined the Internet of Things (IoT). The word “Internet” refers to a network created using interconnectivity devices, while “Things” refers to devices or objects that have internet connection capabilities [3]. With the benefits of IoT in both types, the systems can process, collect, and transfer data without human interference. In this time, diverse applications such as E-banking [4] and emails have replaced the handwritten letters. Processes of purchasing and trading the stocks are increasing every day and connected to an electronic transaction to reduce cost and improve services [5]. These needs have led to expanding the idea of electronic transactions or electronic documents that can be created, processed, stored in the server in an encrypted way, and transmitted via a network. The data stored and transferred over transactions can be confidential and sensitive, protecting these data from third parties and intruders and their malicious actions.

For daily life, handwritten transactions are protected using a handwritten signature, and then authenticated by the parties; the receiver will validate this transaction’s signature. For an electronic transaction, using the digital signature provide this protection. Also, for a handwritten transaction, information and storage are protected using locked rooms or lockers. For electronic transactions, the transaction information is encrypted at the database with cryptographic service, and it decrypted when it is called for use. Database cryptography will protect the stored information from stealing and save data integrity and confidentiality [6]. Organizations started to use various platforms to share knowledge and documents once the problems appear on sharing transactions among employees, tracking them, and knowing their prior status. While the technologies are growing up, it is easy to use internet benefits to share documents and make some communications among employees without leaving their places. Therefore, many problems will be solved with an ETS, adding that cryptography will make the transactions more solid. Simultaneously, the digital signature provides some benefits such as non-repudiation, integrity, and message authentication code [7].

Related work

This section examines the related work on the online systems, some of which being focused on the education, and others on some aspects that are used in our paper to judge the features required in practice. In principle, this system is compared with the currently used hand transactions in terms of the workflow elements, signing capabilities, and position privileges. The following methods are subjected to selected features discussed in the previous section.

Kim *et al*. (2017) [8] proposed digital transactions that depend on the digital signature scheme to provide the security requirements. They designed a heterogeneous integrated digital signature system that supports features that provide contract terms for each user in an IE environment. The system uses digital signature features to provide a system that guarantees independence from heterogeneous platforms when creating digital contract systems, making it easy to extend and maintain the software. This system is web-based and uses only the digital signature in contracts without encrypting the contract itself.

Li *et al*. (2018) [9] proposed a distributed system to share knowledge and services in ecosystems. The proposed framework incorporates block-chain and edge computing development that can meet the security and distributed requirements for separately sharing expertise and services.

Cozart *et al*. (2014) [10] proposed a system that uses a scheme known as disclosing the electronic transaction processing system under the policy. The system consists of a user module and a policy module. The policy module stores the transaction user’s access right policies which decide what user can see or change for a specific transaction. It also stores the user information and contains processors that receive the user requests for processing a transaction. Users can read the needed information through the user’s computer.

Kittur *et al*. (2017) [11] proposed a system providing proper security to the IoT system and avoiding illegal users from access to information system, by using Digital Signatures scheme. For validation of the digital signature, the Batch verification scheme is used to reduce verification time. The proposed method uses different RSA batch verification techniques.

Amin *et al*. (2012) [12] proposed a transaction system used for business fields. The use of transaction system provides three main functions: System runtime functions; that ensure data integrity and availability; System administration functions, which let the users monitor their transactions; and Application development functions, that include access data functions to perform inter-computer communications and manage user interface.

Rattan *et al*. (2010) [13] developed a commerce transaction that provides a safe and effective transaction environment based on the relationship between network security and e-commerce. Public Key Infrastructure (PKI) technology and digital signature are used to provide authentication, confidentiality, and non-repudiation.

The proposed ETS

In principle, ETS is a centralized system. The reason for using centralization, rather than decentralization, is that it fits the government requirements and conditions. When centralization is used, employees can communicate via a LAN network. Admins can control the time to use the system, e.g. making it usable only in official working time. Also, centralized databases do not need to be time-sequenced or keep track of the user’s different states (although the admin can set them up this way if the workflow prefers that). The only requirement is that the database makes data accessible to the software applications that request it. As compared with other systems, the ETS needed to be more convenient for the university environment, from the beginning of transaction issuing to transaction archiving. Many steps are missed in the other systems, such as:

- delivery report using a digital signature.
- transaction tracing using a digital signature.
- Signing priority.
- Database cryptography.
- The large size of the user key pair used for the signing operation.
- A shared platform for seminar announcing.
- User notification in multiple cases.
- Eliminating transaction capability.

Framework and system layers

ETS is designed for university transaction purposes. It takes university needs and policy as a base framework. ETS takes the thanking book as a case study to implement transaction needs, steps, and security needs. Also, ETS provides a shared platform that is used for announcing the seminars. ETS is identified using four layers, each having certain services. Figure-1 depicts the interactions among the layers used in the ETS. A conceptual framework based on IoT and the transactional system is proposed in this paper. Figure-1 and Table 1 show that the ETS consists of four layers: the user, application, security, and, finally, the infrastructure layers.

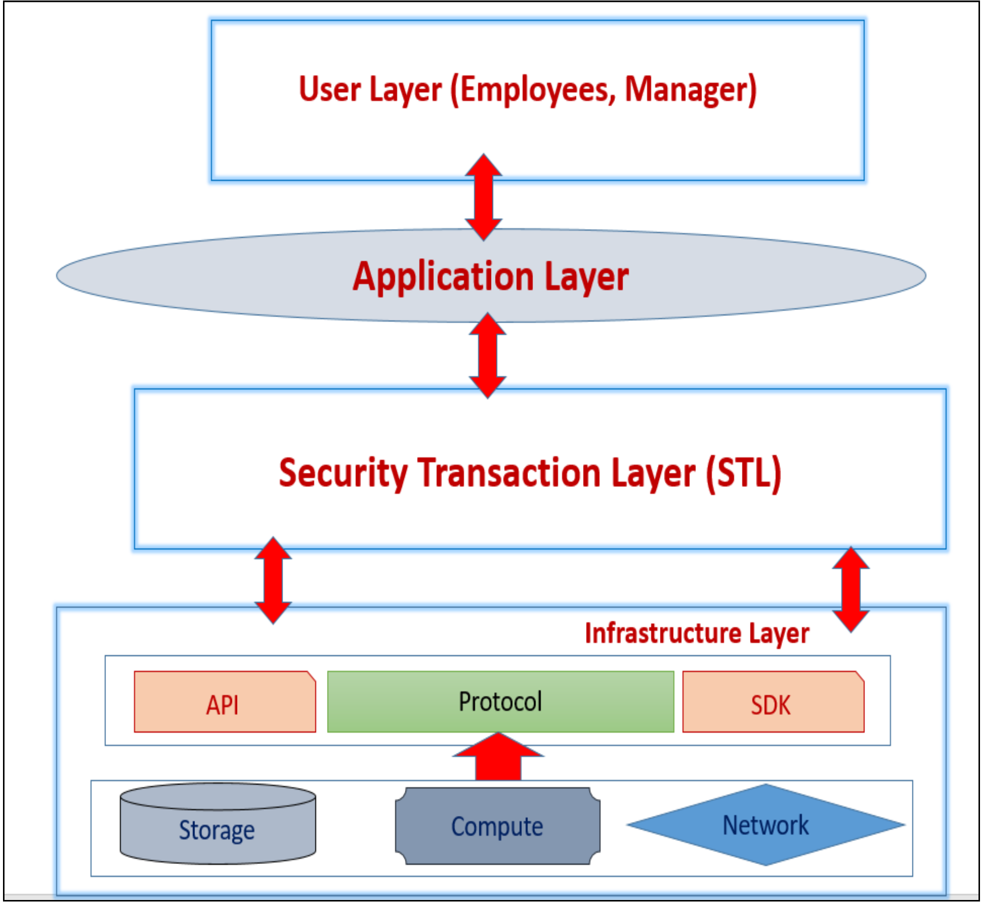


Figure 1-Layers of an IoT-based transactional system.

Table 1-The Functionality of the Four Layers of ETS.

Layer	**Purpose**	**Main component**
User layer	Collects data from employees and different departments to allow the organization to share and access the knowledge and resources provided by the framework.	Manufacturers, suppliers, distributors, logistics companies, data centres, data analysts, etc.
Application Layer	Provides applications to allow the organization staff to share their apps.	Organizations, electronic transaction system application.
Security Transactional Layer	Saves data and information collected, shared, and created from the Application Layer according to the privileges with the needed security.	Cryptography, Authentication, non-repudiation, Integrity**.**
Infrastructure Layer	Provides infrastructure and database to support the different layers.	Computers and servers.

The work of each layer will be discussed, from bottom to top, as follows:

1. Infrastructure Layer: supports the whole system, including the other layers. It provides software and hardware infrastructure for the transactional system. The hardware here is the server that contains all system information, which is to validate the user and transactions. This layer provides methods that include protocols, applications, software development kit (SDK), and interfaces to share transactions and knowledge safely and transparently, while computers are used to exploit these features by the organization staff.
2. Security Transactional Layer: provides security to the application layer. This layer is composed of information collected from the application layer and processed by the application layer. It consists of the security rules that are built according to user privileges. ETS provides this layer to group all security needs and schemes in one layer, which checks user information, signature validation, and database cryptosystem before the user operates the usage of the application layer. This layer is provided only in ETS.
3. Application Layer: provides software and system properties, system application, and service to the employee layer and the organization layer. It works with security and infrastructure layers, which improves data collecting and processing. This layer is a mirror to the other lower layers. It shows the last state of the transactions and users. Also, it is used to insert additional data to the lower layers.
4. User Layer: consists of employees, administrators, and managers that have the responsibility to make a decision and to analyze the collected information through the application layer. The users make use of analyzing collected data, working through the application layer, and then providing various kinds of knowledge, services, and resources for the transactional system.

Security and Privacy in ETS

Transactions in ETS are similar to paper transactions in some aspects, but using a different scheme. The digital signature replaces the handwritten signature in transaction signing and transaction delivery, while the database encryption saves the files as lockers and file keepers. In this section, the security and privacy issues will be discussed as follows.

Digital Signature

A digital signature provides services to the electronic transactional system. The outstanding services include message authentication, message integrity, and message non-repudiation. Moreover, it provides additional services for the system, e.g., it can be used to know how to receive a specific transaction (delivery reports) as well as for notes authentication, notes non-repudiation, and notes integrity. Moreover, the digital signature can provide entity authentication. The digital signature scheme is not sufficient to satisfy some security issues, providing no inherent certainty about the date and time at which a transaction was signed.

For this reason, there are services attached to a digital signature, which are named the Time-Stamp supporting transaction workflow systems [14]. The digital signature has multiple schemes. In this paper, the proposed method uses the secure hash algorithm (SHA3) and the RSA algorithm.

The functions of the SHA3 family operate on binary data. In ETS, the SHA3-512 was used according to the key size, which makes it hard to break [11] [15]. For the electronic transactional system, the cryptographic hash function improves the efficiency and security of the digital signature scheme because the hash value is digitally signed instead of the plain message itself. Also, SHA3 provides a message authentication code (MAC) service, while RSA is an asymmetric cryptosystem used in ETS for signing and verification purposes using the key pair [16].

The steps used for signing and verifying the digital signatures are shown in Figure-2 and Figure-3.

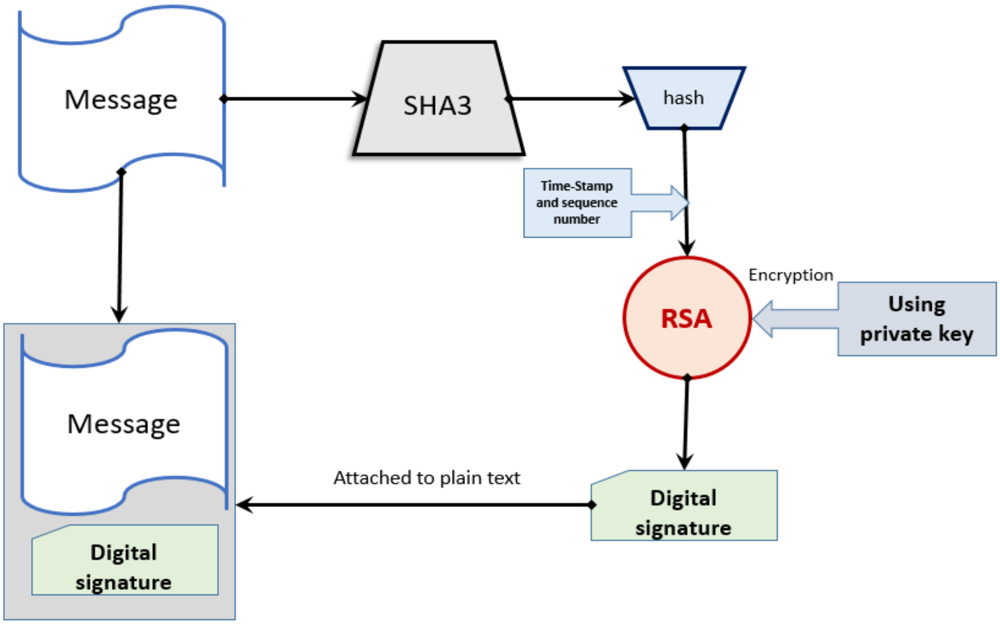


Figure 2-The digital signature signing scheme.

The sender sends the message with signature, while the signature is the encrypted hash value of the message with a time-stamp and sequence number. In the signing level, the private key is used for encryption. At the transaction receiver side, the employee receives the transaction with the digital signature, the operation of verification will be done by calculating the hash value of the received message, the digital signature attached is decrypted, and the results are compared.

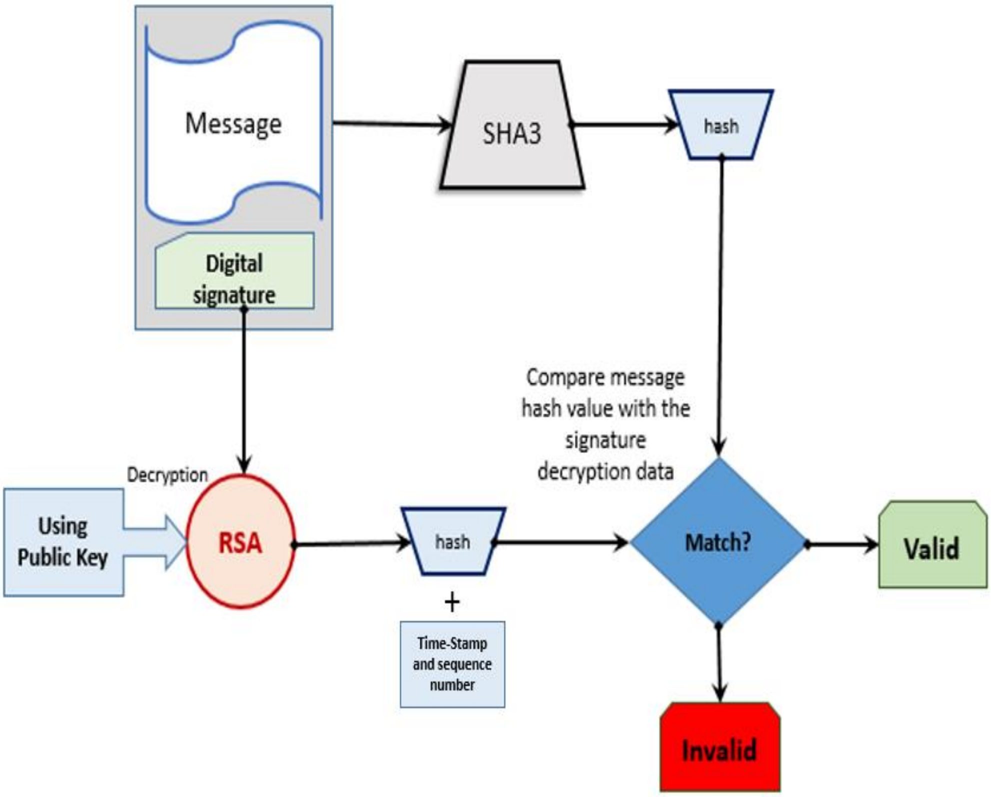

Message
Digital signature
SHA3
hash
Compare message hash value with the signature decryption data
Decryption
Using Public Key
RSA
hash
+
Time-Stamp and sequence number
Match?
Valid
Invalid

Figure 3-The digital signature verification process.

The signing operation and verification process will be made at STL.

Features of the ETS

- **Secure login**: user's username and password should be registered in an encrypted way in the database. The login is done after checking the server name and its database. The username is unique, and the password should be more than eight characters.
- **Portability:** The electronic transactional system can run on any platform fashion (software and hardware). While the ETS consists of two parts: client-side and server-side. The server part is the place where the transaction is created and processed, whereas the client part represents the employees who start to issue a transaction and sign it with their digital signature. These parts can be built as a web-based application.
- **Transaction Resumption Capability:** While the transaction is created and transferred through the system channel, it will be directly saved in the transaction database, which will protect it from damage or loss. The resumption capability for a created transaction will make the employees able to complete the transaction progress.
- **Multi-Instructor**

The electronic transactional system needs to be reliable and should have multi-instructor features, which make each employee, has his/her privileges and access. ETS should consist of a manager, employees, and the Audit-Committee. The managers control the system and the opportunities of each employee. The employees are responsible for creating a transaction, reading it, making an action if needed, and sending it to each other. At the same time, the Audit-Committee is responsible for checking the rightness of the transaction content. The database architecture is shown in Figure-4.

- **Transaction elimination**

ETS provides a unique service, which is the transaction elimination as transaction elimination in the university environment. As a university staff structure, the aduit-commetie is responsible for checking the validation of transaction content. When a user receives a transaction and disapproves it, the transaction will move to the aduit-commite with user notes, where a decision to eliminate this transaction can be made.

- **User notification**

Other systems have multiple ways to send a notification to users. ETS generates the most practical way for alarming the user to open the ETS and for transaction signing. Firstly, when users read specific transactions, ETS registers a read status for the logged user. When the user neglects to open the system for two days, ETS will send an email to the delinquent user and send a notification to the Audit-Committee to take the necessary action.

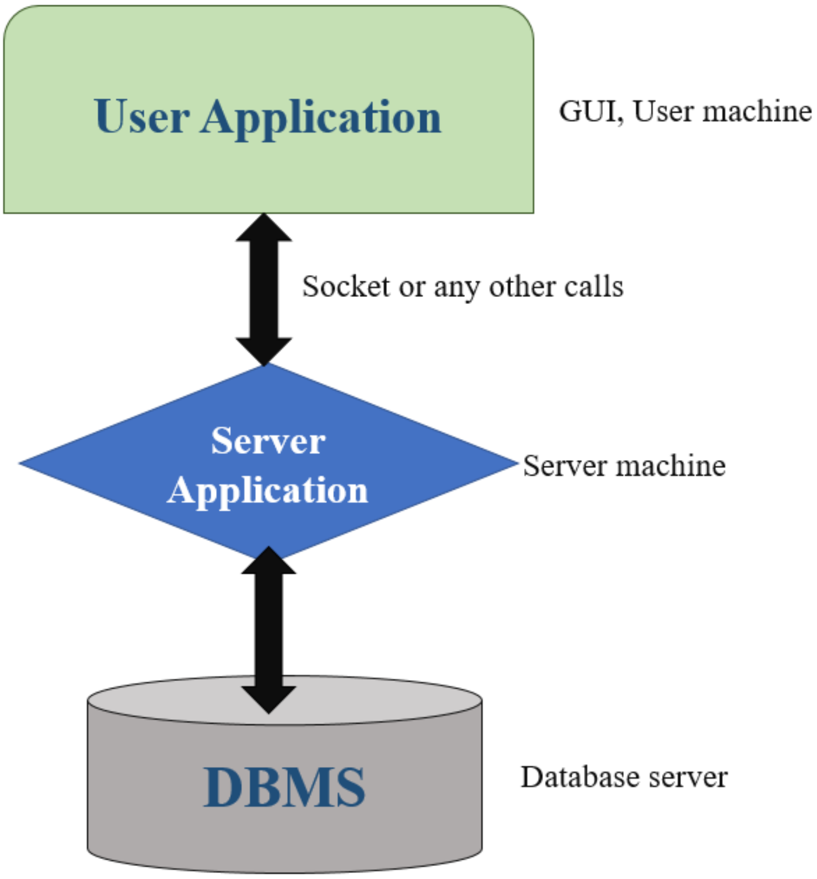


Figure 4-The database architecture.

The ETS implementation

Actors in ETS

As in the previous sections, we proposed implementing ETS in the university rather than the current paper-intensive system used. To do that, ETS separates the university staff according to positions and gives each of them position-specific access rights and privileges, as follows:

- The University President and his/her assistant: can read all the issued transactions, issue new transactions, and sign each issued transaction in the university.
- The Dean and Associate Dean: can read the entire issued transactions exclusive to the college, issue new transactions, and sign each issued transaction subjected to the college.
- The Head of the Department: can issue new transactions and should sign each transaction subjected to the department.
- The Professor: can issue a request for a thank-you letter. This letter is sent to the scientific committee and audit-committee to validate the information and send it to the University presidency and college deanship to decide about the request.
- Scientific-Committee: can sign the issued requests and transactions that need their approval.
- Audit-Committee: responsible for transaction status and can eliminate transactions in some cases. Also, the Audit-Committee can sign the transaction that needs its approval.
- Department and postgraduate decision-makers: can post a new seminar date and, after finished, they can register attendance names.
- Employees: can issue new requests and sign specific cases.
- Admin of system: Change the system settings, such as key size, email setting, and database encryption-key size for AES.

Each of the listed positions should sign a delivery report when they are mentioned in a transaction.

Architectural Design of ETS

The server-side and employee side are the central portions of the ETS. The server-side controls ETS operation and consists of a database, network, and graphic user interface (GUI). The employee side consists of user machines, temporary storage, GUI, and network. The server and the user play the role of the protocol handlers of ETS and are connected via a network. Figure-5 shows the server and user sides and explains the control of both of them.

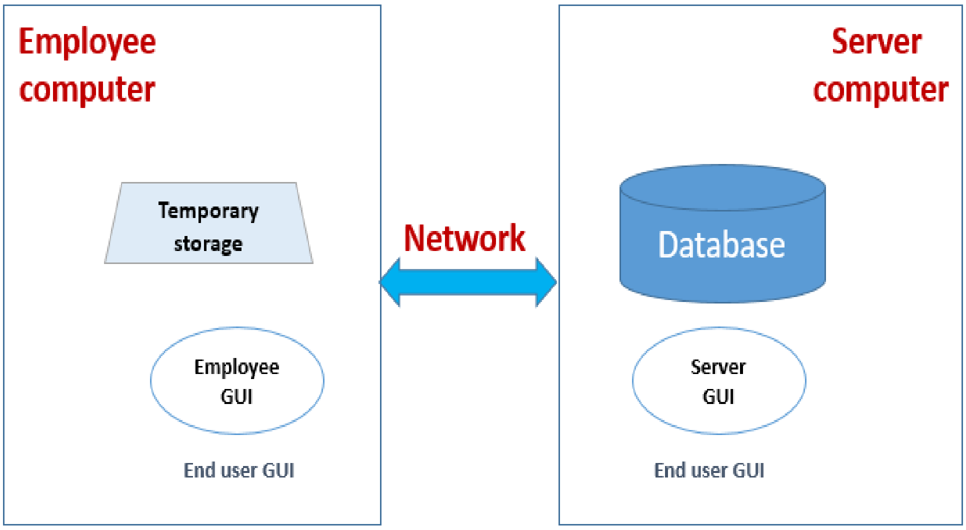


Figure 5-The ETS block diagram.

Database Security

The database contains a group of tables used in the server-side operation phases and maintained by special programs called Database Management Systems (DBMSs), such as the Structured Query Language (SQL) server that is used in the ETS database. The database uses the Advanced Encryption Standard (AES) algorithm to encrypt the database information, with a key length of 256 bit. Figure-6 shows the ETS database entity diagram and the relationships.

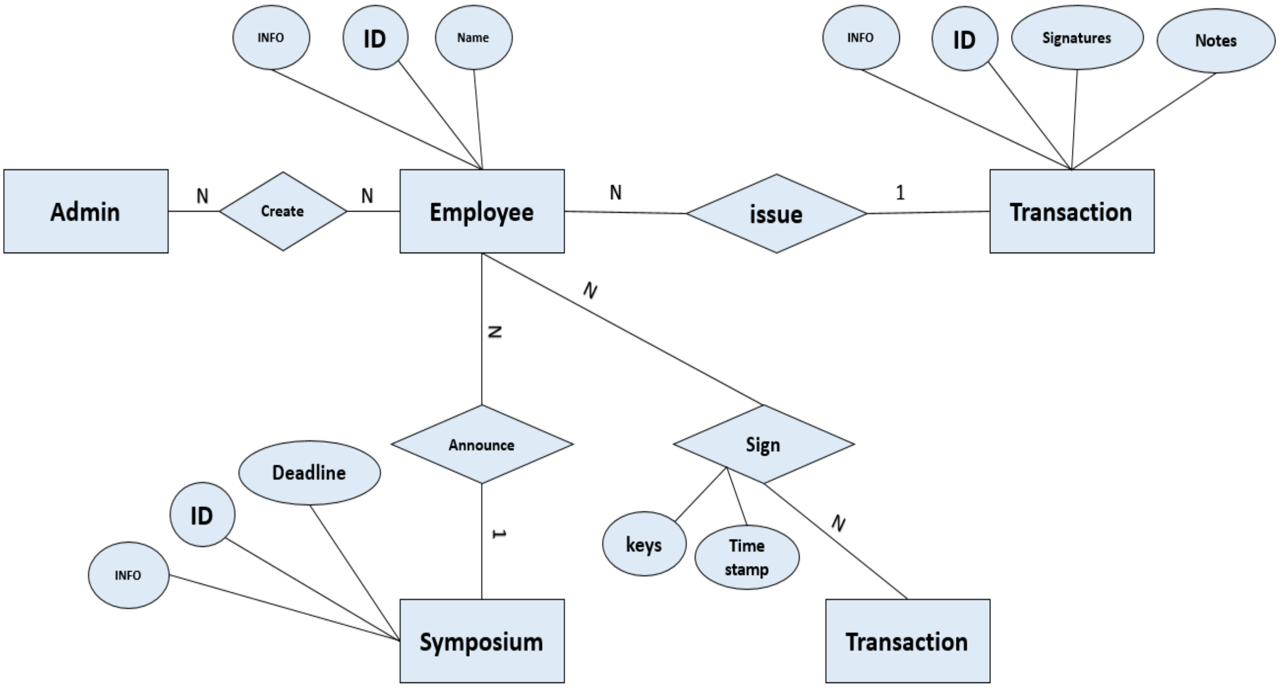


Figure 6-Database Entity Diagram

Networking in ETS

ETS is a network-based system. It runs on a connected server with employee machines over a network. When logging in, the employee sends their user name and password to the server on the server port and handle each connection in a separate thread. An authentication check happens in the server and then sends back a reply as verified or not. When the response is a grant, the server sends the transactions that need the user's digital signature, if any, or displays the ETS services. When the employee chooses to issue a new transaction and digitally signs it, the user collects the transaction information and sends it to the server for checking and granting. In the end, the final transaction is displayed to an employee through GUI. The sequence diagrams for the ETS operation phases are depicted in Figure-7.

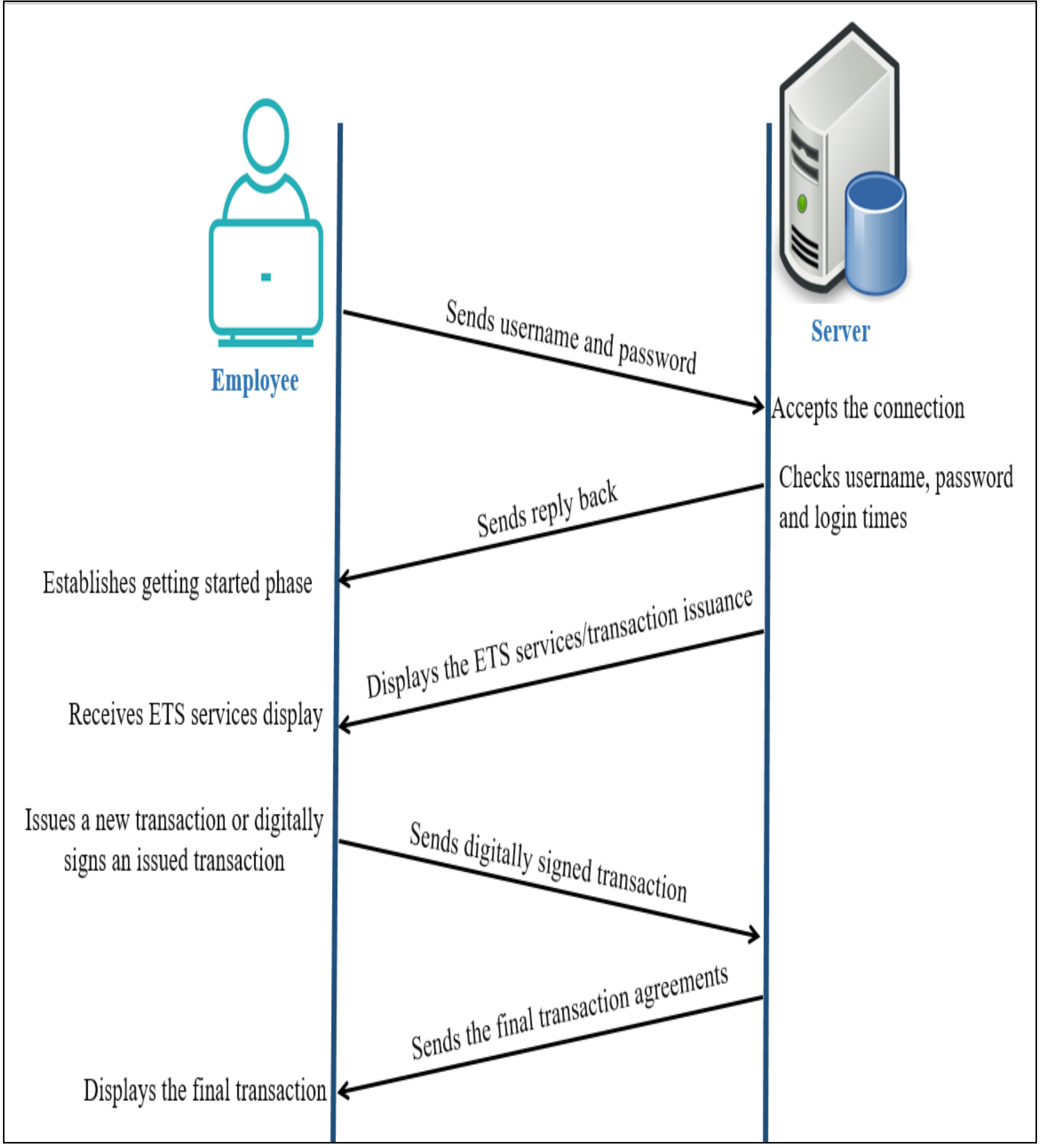

Employee
Server
Sends username and password
Accepts the connection
Checks username, password and login times
Sends reply back
Establishes getting started phase
Displays the ETS services/transaction issuance
Receives ETS services display
Issues a new transaction or digitally signs an issued transaction
Sends digitally signed transaction
Sends the final transaction agreements
Displays the final transaction

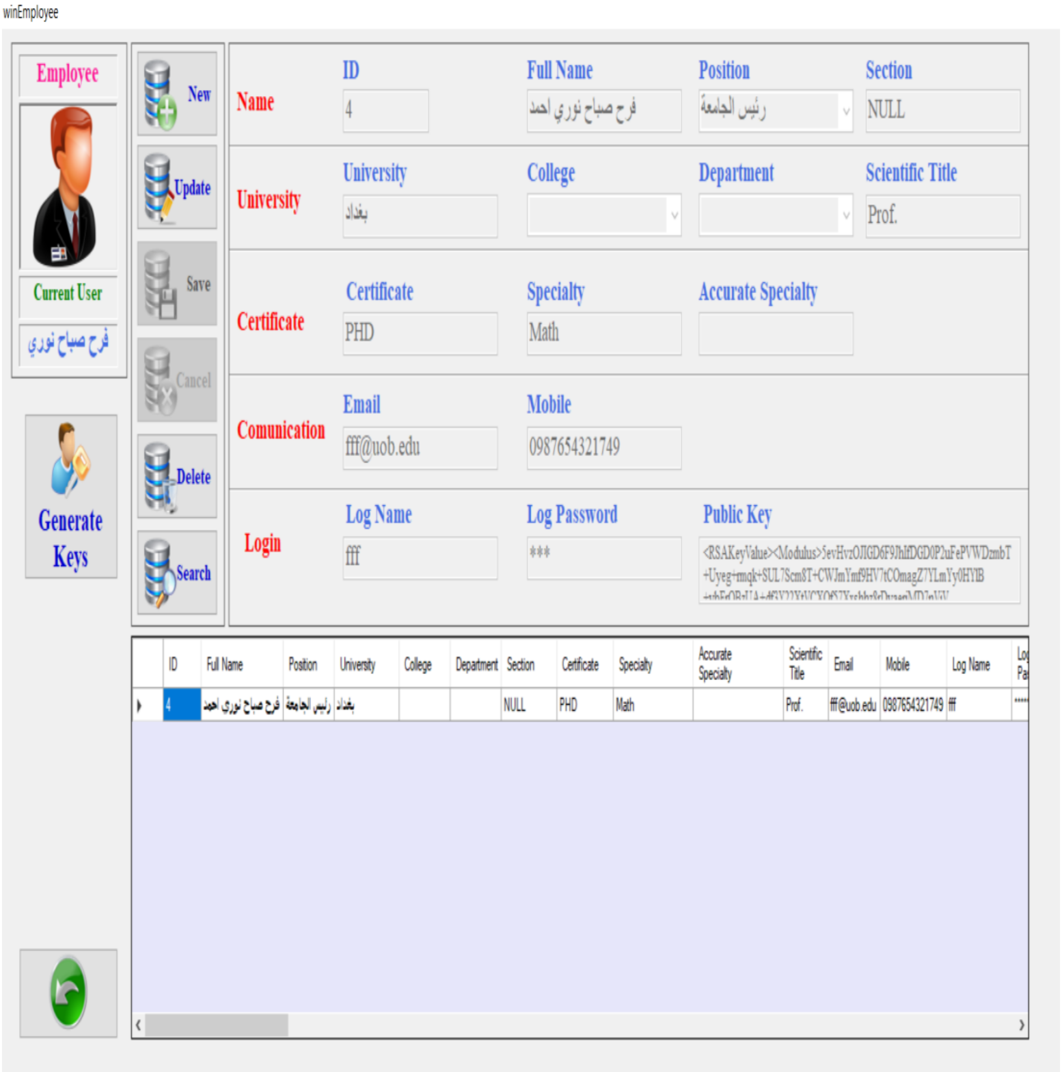
Figure 7-Networking between the employee agent and the server agent.

Implementation of ETS

The proposed ETS was implemented using Visual Studio 2015 (C#) for GUI and SQL-Server 2016 and Visual Studio 2016 for the database management.

ETS initialization

The administrator has a privilege to create a new user according to the employee's information issued by the corporation. Each user has a username, password, public and private keys, and privilege according to his/ her position. Figure-8 shows the process of employee account creation.



Name	ID: 4	Full Name: فرح صباح نوري احمد	Position: رئيس الجامعة	Section: NULL
University	University: بغداد	College:	Department:	Scientific Title: Prof.
Certificate	Certificate: PHD	Specialty: Math	Accurate Specialty:	
Comunication	Email: fff@uob.edu	Mobile: 0987654321749		
Login	Log Name: fff	Log Password: ***	Public Key: <RSAKeyValue><Modulus>5evHvzOJIGD6F9JhlfDGD0P2uFePVWDzmbT +Uyeg+mqk+SUL7Scm8T+CWJmYmf9HV7tCOmagZ7YLmYy0HYIB	

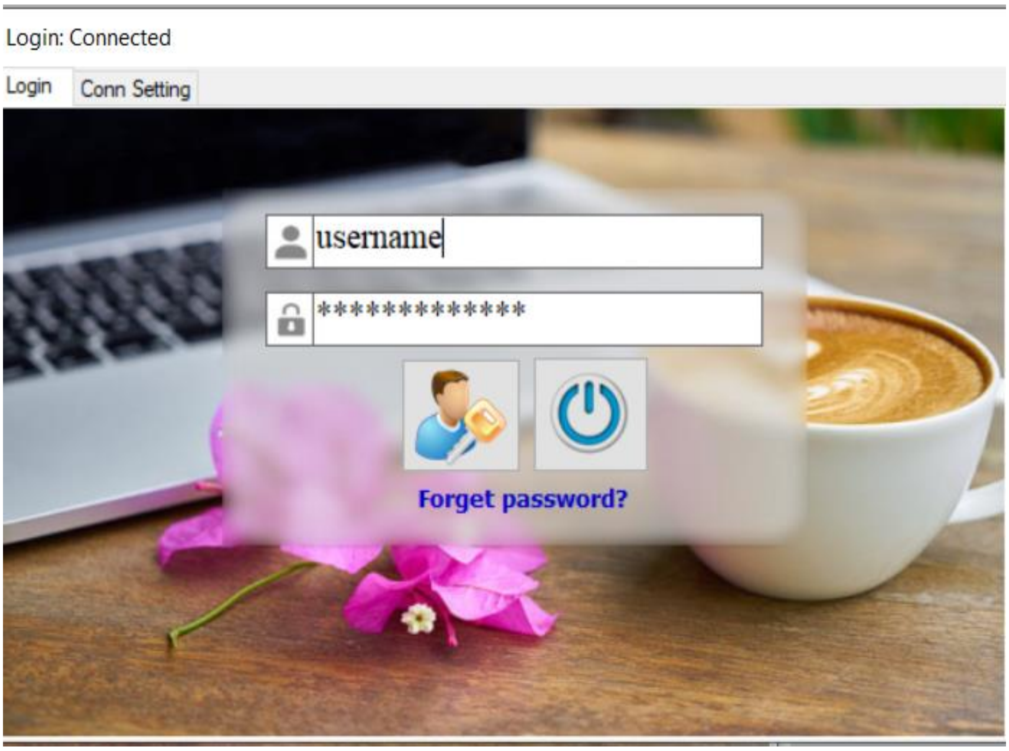
	ID	Full Name	Position	University	College	Department	Section	Certificate	Specialty	Accurate Specialty	Scientific Title	Email	Mobile	Log Name	Lo Pa
▸	4	فرح صباح نوري احمد	رئيس الجامعة	بغداد			NULL	PHD	Math		Prof.	fff@uob.edu	0987654321749	fff	****

Figure 8 - The account creation window.

ETS phases

The ETS networking has a mutual authentication between user and server. First, the employee should be connected to the server and the database specified for the ETS. According to government transaction processing, the ETS has six phases: login phase, transaction issuance, transaction signing or authentication phase, transaction validation, transaction tracking, and transaction storage.

1. **Login phase**: The user enters the username and password created by the administrator, as shown in Figure-9. If the information entered is false after five trials, the user will be blocked from the login for thirty minutes, and an email message will be sent with the new password. Users can see their information by clicking on the employee button in the ETS main GUI and can change an only username, password, and signing keys. The administrator can see the complete employee information, update them, and remove them.


Login: Connected

username

****

Figure 9-The GUI of ETS for login.

2. **Issuance phase:** Figure-10 shows the primary services that ETS provides to the user. The “Issue” button allows the user to issue a new transaction, as shown in Figure-11, or news according to the user privileges, digitally signs the issued transaction and specifies whom to approve and how to see this transaction. The seminar button allows the department and graduates’ rapporteurs to make seminar advertising and attendance registration more comfortable and practical for university usage.seminar and seminar attends information window shown in Figures- 12 and 13.

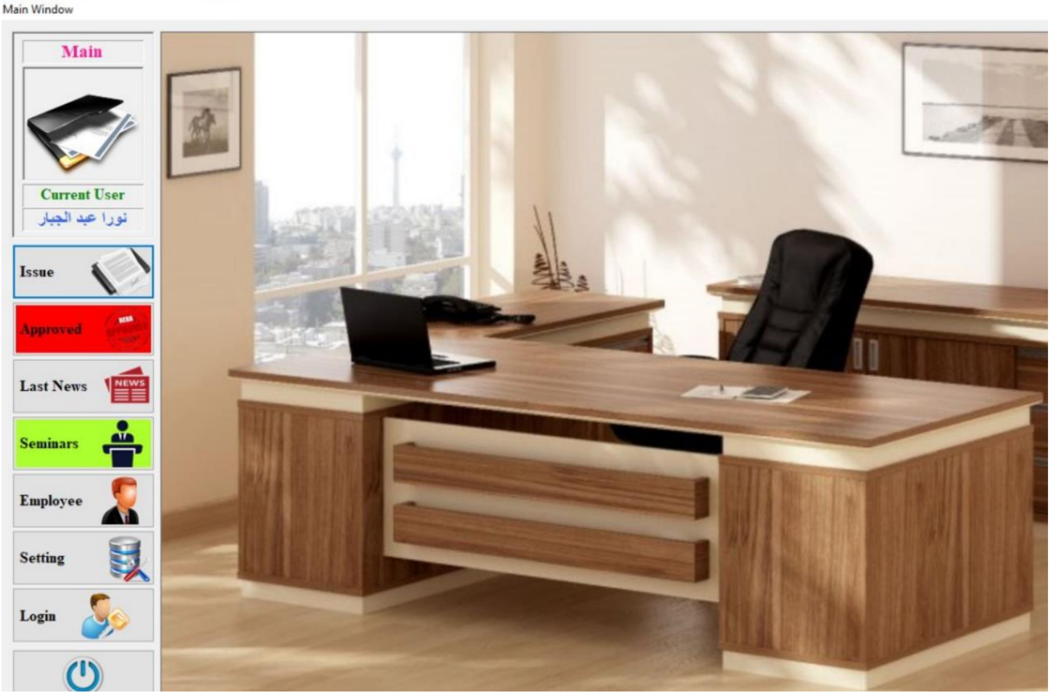
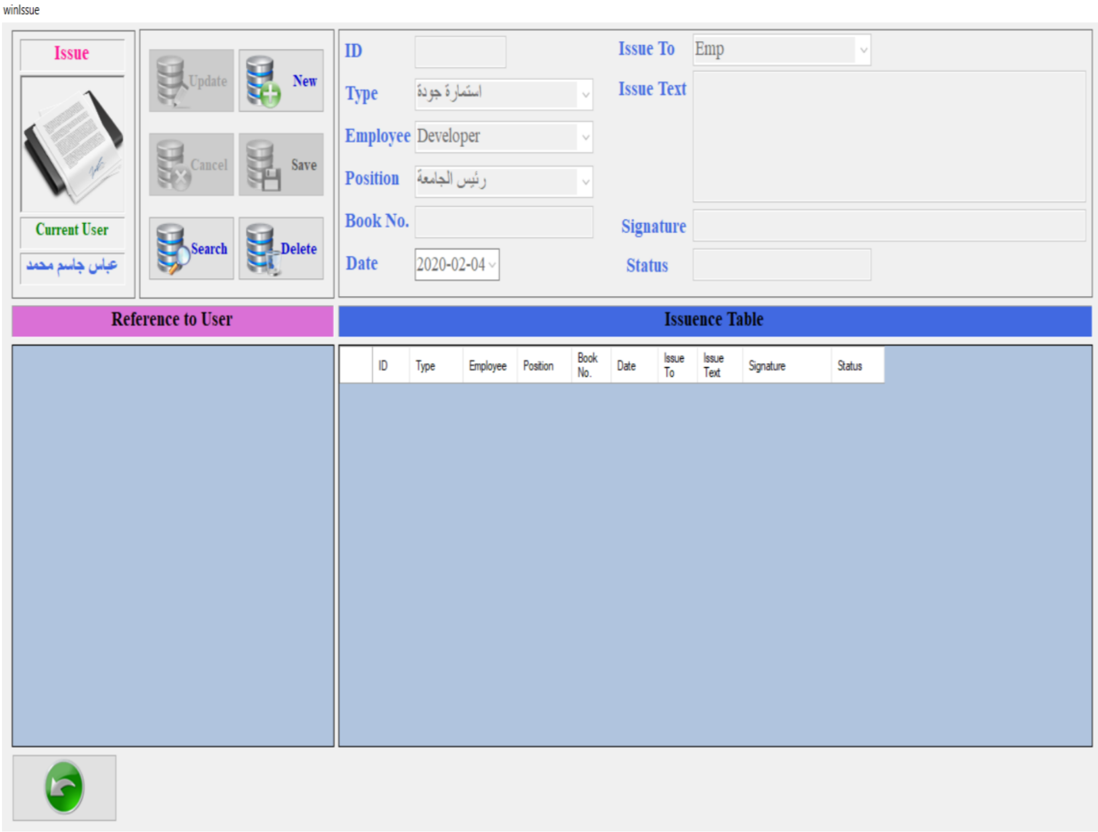

Current User
نورا عبد الجبار

Figure 10-ETS main services GUI.

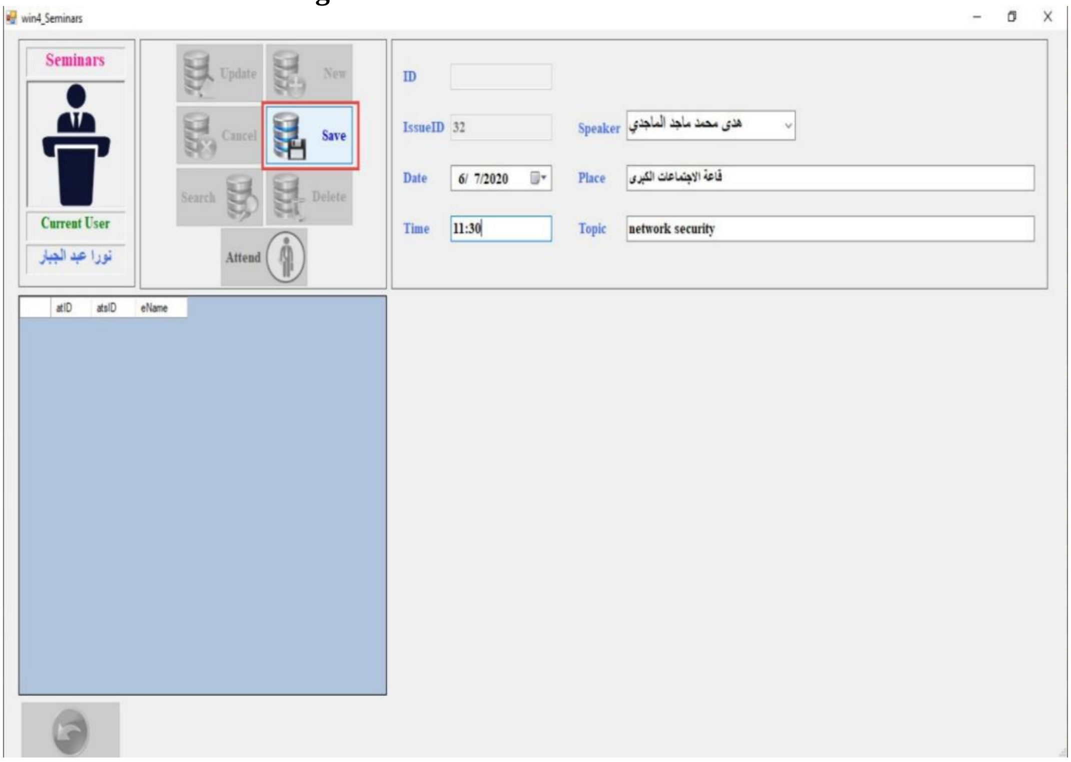


Current User: عباس جاسم محمد

ID:
Type: استمارة جودة
Employee: Developer
Position: رئيس الجامعة
Book No.:
Date: 2020-02-04
Issue To: Emp
Issue Text:
Signature:
Status:

	ID	Type	Employee	Position	Book No.	Date	Issue To	Issue Text	Signature	Status

Figure 11-The GUI for the ETS issuance.



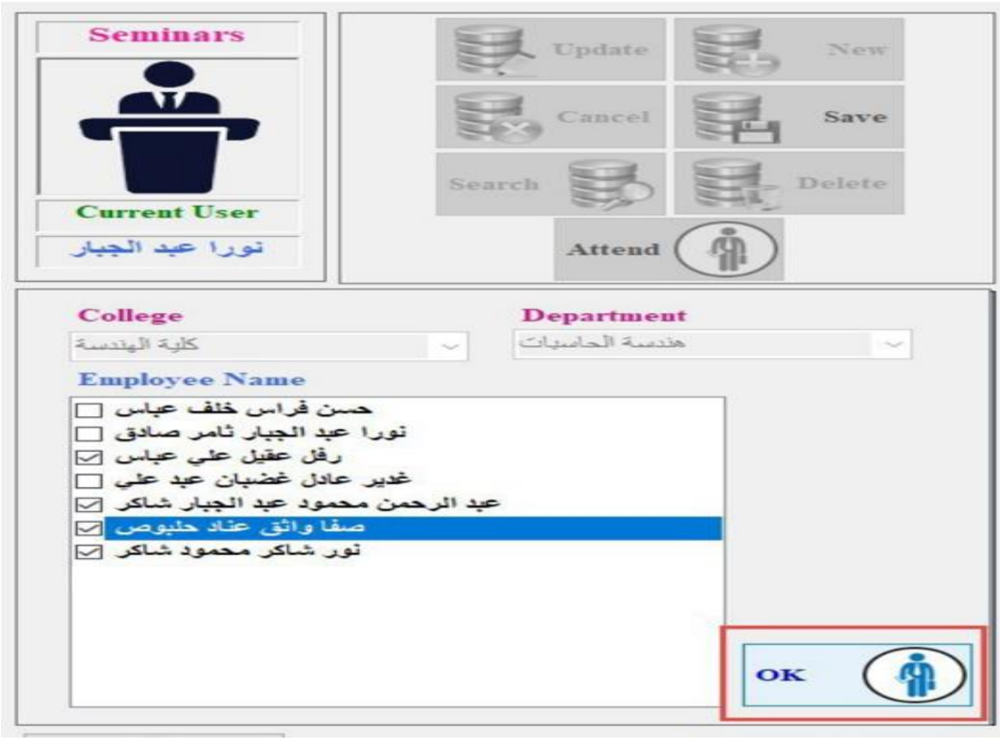
Current User: نورا عبد الجبار

ID:
IssueID: 32
Speaker: هدى محمد ماجد الماجدي
Date: 6/ 7/2020
Place: قاعة الاجتماعات الكبرى
Time: 11:30
Topic: network security

	atID	atsID	eName

Figure 12-Seminar issuance Frame.

When a user selects to announce for a seminar, he/she should have an access right to do that. If the user already has this access right, the announcement will be stored in the database with user digital signature and appear for all users. After the seminar is finished, the user should enter the names of the attendees, as shown in Figure-13.



Current User: نورا عبد الجبار

College: كلية الهندسة

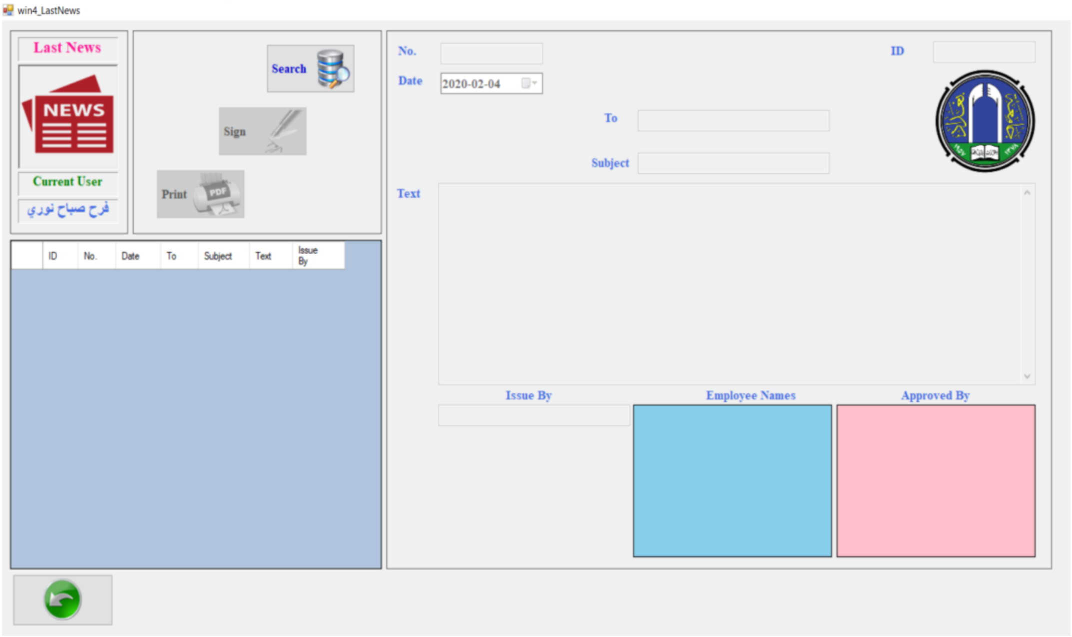
Department: هندسة الحاسبات

Employee Name

- ☐ حسن فراس خلف عباس
- ☐ نورا عبد الجبار ثامر صادق
- ☑ رفل عقيل علي عباس
- ☐ غدير عادل غضبان عبد علي
- ☑ عبد الرحمن محمود عبد الجبار شاكر
- ☑ صفا واثق عناد حلبوص
- ☑ نور شاكر محمود شاكر

Figure 13- Seminar Attendance Frame

3. Authentication phase: Users can read the last transactions specified to them, and the issued news by clicking on the Last News button. Users cannot see the transaction subject before digitally signing for opening the transaction subject. Figure-14 shows the last news window. The Approve button also cannot see the transaction subject before digitally signing for opening it, as shown in Figure-15. After opening it, the user can approve the transaction, and the digital signature will be added for the improvement list. The notes are attached to the specific transaction. The signing operation is conducted with importing the private key that is saved in the user computer. Each time the user imports the private key for signing the ETS, he/she is asked for the account password to prevent the system from the masquerade.

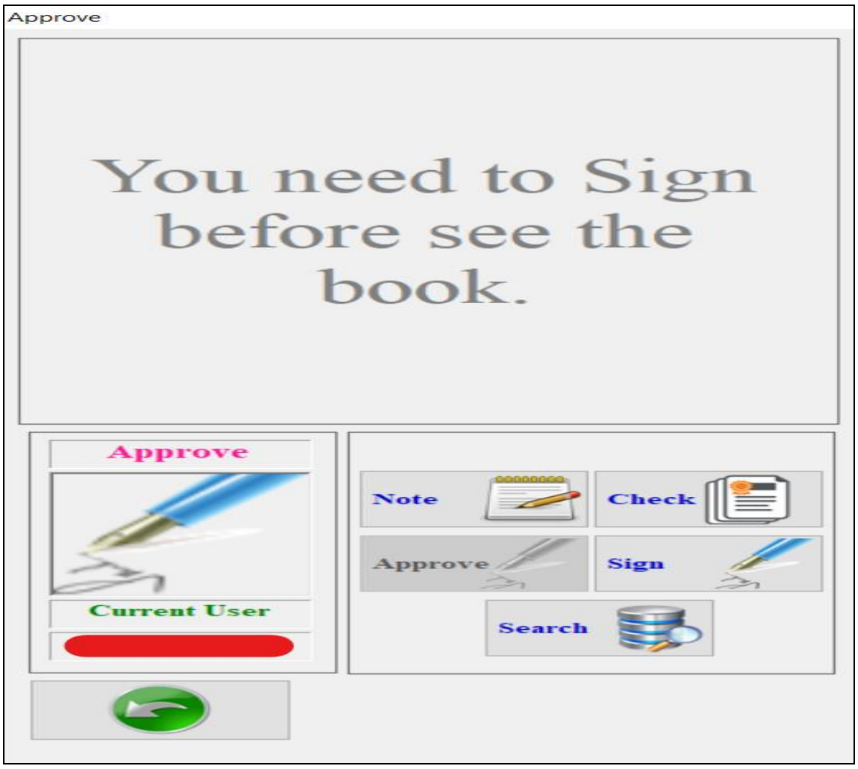


Current User: فرح صباح نوري

Date: 2020-02-04

	ID	No.	Date	To	Subject	Text	Issue By

Figure 14-The ETS last news GUI.


Approve

You need to Sign before see the book.

Figure 15- The ETS approval GUI.

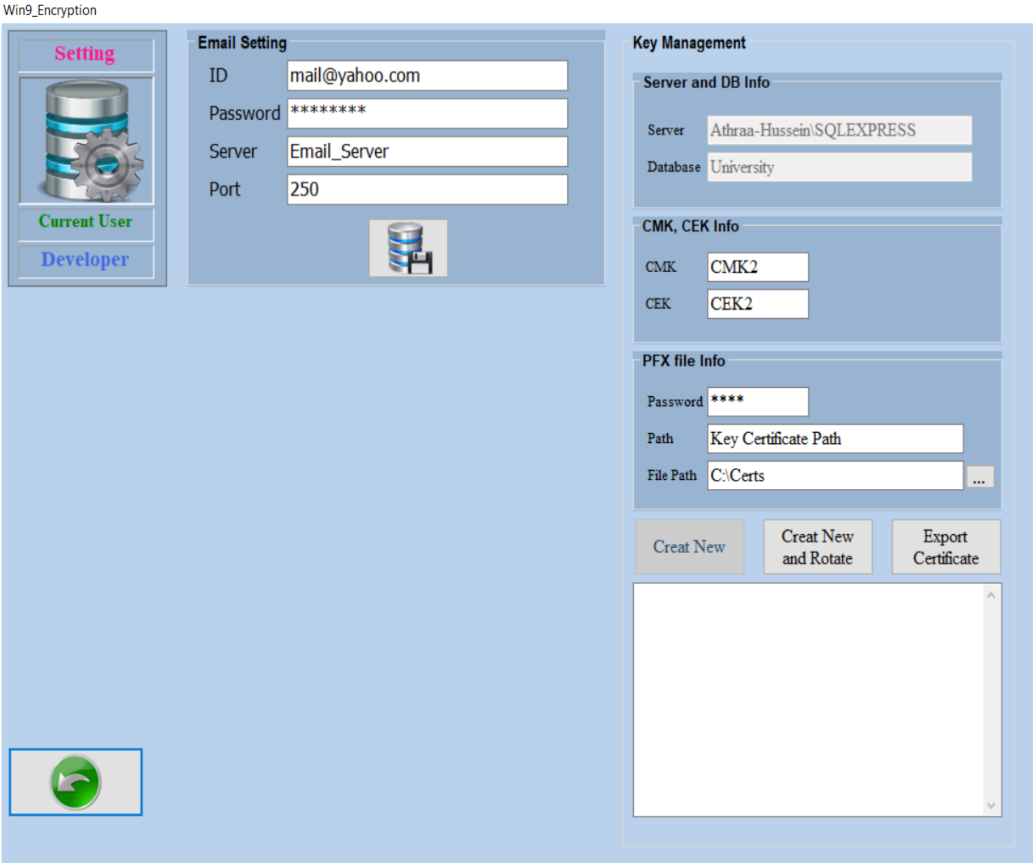
4. Validation phase: The ETS system uses the RSA and SHA3-512 for signing the operations as mentioned previously. Also, the verification progress is made to check the original information with the decryption of the signature. In ETS, this is performed by clicking the check button, as shown in Figure-15.

5. Transaction Tracking: Knowledge of negligence in the transaction context, the system displays the received transaction history to all the persons mentioned in the transaction and sends an email message to the user if he/she has neglected the transaction for more than two days.

6. Transaction Storage: After signing the transaction by all the mentioned employees, the whole transaction, notes, and signatures will be saved in the database, and the users who have access to specific transactions can search and print them if needed.

The setting of email and database encryption key

The setting of the email that is used for user notification is accessible exclusively by the administrator. The administrator can edit it if there is any change in the email server, like the in-coming/out-coming server, port numbers, email ID, and password. The admin’s key for database cryptography can be changed by clicking “Create new and Rotate” button. This key will turn to the original value and re-encrypt the database with the new key. The database key management certificate should be exported and installed on the user’s computers to allow them to communicate with the server using the database key for encryption and decryption. The setting window is shown in Figure-16.



Win9_Encryption

Email Setting

ID: mail@yahoo.com

Password: ********

Server: Email_Server

Port: 250

Key Management

Server and DB Info

Server: Athraa-Hussein\SQLEXPRESS

Database: University

CMK, CEK Info

CMK: CMK2

CEK: CEK2

PFX file Info

Password: ****

Path: Key Certificate Path

File Path: C:\Certs

Figure 16-The ETS setting GUI.

Conclusions

This paper proposes an ETS with a digital signature scheme, based on RSA and hash algorithm, and database encryption by the symmetric algorithm, i.e. AES. This system is designed for university environment usage. The ETS overcomes the drawbacks in the existing systems used for transactions in many institutions, such as the key size, database security, and the needed workflow and infrastructure. This system is useable and can be developed by building other types of transactions, using programmed classes to create models of transactions with their roles and privilege. The comparison of the desired features is missing in the reviewed systems, as shown in Table-2. Combining these desired features in the proposed system is the significant contribution of this paper. The comparison showed the advantages of ETS over the existing systems. The elected services that were accomplished shown in Table 2. The ETS provides a secure login that prevents the system from unknown users.

Moreover, it is portable to desktop operating systems. It has a resumption capability that allows users to continue their work because of the server's transactions. The ETS uses the digital signature scheme to provide digital signature services for the transactions, which are: message authentication, non-repudiation, integrity, and additional services, such as delivery reports, entity authentication. Time stamping supports the digital signature by recording the information creation time and signing time. The ETS monitors the status of the created transactions when the user neglects the transaction for more than two days; the ETS sends an email to the delinquent in transaction workflow and shows the transaction creator and the mentioned users the last status of the transaction. The ETS uses an encrypted database using the AES scheme with a key length of 256 bits to prevent the stored data from stealing and illegal use. As a part of future work, we are currently working on deploying the product at the University of Baghdad to perform Beta testing and adopting different electronic transactions.

Table 2- Comparison among the Related Systems According to the Services Provided by Online Systems and Digital Signature Based Systems.

✔(Supported Feature) **✖(Not Supported Feature)**	**Elected Features**												
	System general services					**Digital signature services**					**Additional services**		
Online systems /digital signature-based systems	Secure Login	Resumption Capability	Multi-Instructor	Portability	Application-based, web-application or Hybrid	Message Authentication	Entity Authentication	Integrity	Non-Repudiation	Time Stamping	Document tracing	Database encryption	Transaction rollback
Heterogeneous Integrated Digital Signature System for Ensuring Platform Independence [8]	✖	✖	✖	✔	Web-Based	✔	✔	✔	✔	✖	✖	✖	✖
A cross-enterprises knowledge and services exchange framework based on block-chain and edge computing [9]	✔	✖	✔	✔	Hybrid	✖	✖	✖	✖	✖	✔	✖	✖
Electronic Transaction System [10]	✔	✖	✔	✔	Web-Based	✖	✖	✖	✖	✖	✖	✖	✖
Fast Verification of Digital Signatures in IoT [11]	✔	✖	✖	✖	Application-based	✔	✔	✔	✔	✖	✖	✖	✖
Business Transaction Processing System [12]	✔	✖	✖	✔	Web-based	✖	✖	✔	✖	✖	✖	✖	✖

E-Commerce Security using PKI approach [13]	✔	✖	✖	✔	application-based	✔	✔	✔	✔	✖	✖	✖	✖
ETS	✔	✔	✔	✔	Web-application	✔	✔	✔	✔	✔	✔	✔	✔

References

1. Abdullah, K. E. and Ali, N.H.M. **2018**. A Secure Enhancement for Encoding/ Decoding data using Elliptic Curve Cryptography. Iraqi Journal of Science, **59 (1A)**: 189-198.
2. Harba, E. S. I. **2018**. Advanced Password Authentication Protection by Hybrid Cryptography &Audio Steganography. Iraqi Journal of Science, **59 (1C)**: 600-606.
3. Younis, M. I., Younis M. F., Abed M. M. and Alsewari, A. A. **2020**. Development of an Attendance System Based on Cloud / Fog Computing with Data Recovery Capability. *Iraqi Journal of Science*, **61(5)**: 1190-1201.
4. Kaushal, V., and Balaini, A. **2016**. E-Banking: Challenges and Issues, Hill Quest, **3 (3)**: 69-73.
5. Al-Abdallah, G. M. and Bataineh, A. Q. **2018**. Social Networking Sites and Fashion E-Purchasing Process. *Journal of Business and Retail Management Research* (JBRMR), **13(2)**: 1-11.
6. Almutairi, A. H. and Alruwaili A. H. **2012**. Security in Database Systems. *Global Journal of Computer Science and Technology Network, Web & Security*, **12(17)**: 1-7.
7. Stallings W. **2017**. *Cryptography and Network Security Principle and Practice*. 7th edition, Pearson Education.
8. Kim, H-J., Yoon, J. I., Jang, Y. and Park, S. **2017**. Design of Heterogeneous Integrated Digital Signature System for Ensuring Platform Independence, the 4th IEEE International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali: 1-4.
9. Li, Z., Wang, W. M., Liu, G., Liu, L. and He, J. **2018**. Toward Open Manufacturing a Cross-Enterprises Knowledge and Services Exchange Framework Based on Blockchain and Edge Computing. *Industrial Management & Data Systems*, **118(1)**: 303-320.
10. Dennis Cozart, Lorcan McGuinness, and Michael Peterson. **2014**. Electronic Transaction System, United States Patent, sheet 1 to 5.
11. Kittur, A. S., Jain, A. and Pais, A. R. **2017**. Fast Verification of Digital Signatures in IoT. Thampi et al. (Eds.): Security in Computing and Communications, *Communications in Computer and Information Science*, **746**: 16–27.
12. Amin M.B., Alauddin M.D. and Azad M.M. **2012**. Business Transaction Processing System. *International Journal of Computer Information Systems*, **4(5)**: 11-15
13. Rattan, V., Sinha, M., Bali, V. and Rathore, R. S. **2010**. E-Commerce Security using PKI Approach. *International Journal on Computer Science and Engineering*, **2(5)**: 1439-1444.
14. Younis, M. I., Abdulkareem, H. F. and Ali, H. M. **2015**. Construction of Graduation Certificate Issuing System Based on Digital Signature Technique. *Journal of Engineering*, **21**(6): 15-36.
15. Pritzker, P. and May, W. **2015**. Announcing the SHA-3 Standard: Permutation-Based Hash and Extendable Output Functions. Federal Information Processing Standards Publication 202, NIST.
16. Childs, L.N. **2019.** RSA Cryptography and Prime Numbers. In: *Cryptology and Error Correction, An Algebraic Introduction, and Real-World Applications*. Springer, Cham.