# Employ technology of Bluetooth in the service of the E-government to ensure the security of data-reciprocal which use for this technique

**Lecturer / AbdulIlah Ismael Jarallah**

Diyala Univ. / Basic Education Col. / Computer Sc. Dept.

Abdulilahismael1964@yahoo.com

## Abstract

Objective of this research is an investment Bluetooth in the exchange of information (send and receive information) as an electronic service on numerous projects including e-government that this technique provides users with easy exchange of information in several locations at the same time and at very low cost. Because of global interest in this technology in the necessity used in many electronic devices that supplied this technology, especially computers and accessories in addition to mobile phones and many devices video and audio and the fact that this service information is exchanged wirelessly any transmission of information between electronic devices via Ether making this information is subject to receipt by the people their devices equipped with Bluetooth had to be thinking of finding a means of keeping those data sent through the building security system using one codecs complex was chosen as the encryption system flowchart (Stream Cipher) for the purpose of encryption texts clear before sending over the air has owned this high degree of complexity of the system from which you can send any data to be exchanged within the geographical area, taking into account the capacity and access point to the desired location by the presence of a number of alternatives for the purpose of strengthening the signal and access to the farthest place. With this system off the message and received points where they were building an address (Protocol) for both parties in order to enable the sender of encrypted data and also enables the recipient encrypted data from solved in an easy way without making a lot of effort.

## Keywords :

Blutooth Technology, E-Government . Encryption Algorithm, Decryption Algorithm, cipher text, Plain text, Shift Register, Basic Key

# توظيف تقنية البلوتوث في خدمة الحكومة الالكترونية وضمان امنية البيانات المتداولة عبر هذه التقنية

**من قبل: م. عبدالاله إسماعيل جارا لله**

جامعة ديالى/ كلية التربية الأساسية / فسم الحاسبات

Abdulilahismael1964@yahoo.com

**Employ technology of Bluetooth in the service of the E- government to ensure the security of data-reciprocal which use for this technique**

**AbdulIlah Ismael Jarallah**


## خلاصة البحث

هدف البحث هو استثمار تقنية البلوتوث في تبادل المعلومات (إرسال و استلام المعلومات) كخدمة الكترونية في مشاريع عديدة من بينها الحكومة الالكترونية كون هذه التقنية توفر لمستخدميها سهولة تبادل المعلومات في مواقع عديدة في آن واحد وبكلفة واطئة جداً . وبسبب الاهتمام العالمي في هذه التقنية في ضرورة استخدامها في العديد من الأجهزة الالكترونية التي زودت بهذه التقنية و خاصة الحاسبات و ملحقاتها إضافة إلى أجهزة الهواتف النقالة و العديد من الأجهزة الفيديوية و الصوتية و لكون هذه الخدمة يتم تبادل المعلومات لاسلكياً إي انتقال المعلومات بين الأجهزة الالكترونية عبر الأثير مما يجعل هذه المعلومات عرضة للاستلام من قبل الأشخاص الذين أجهزتهم مزودة بتقنية البلوتوث كان لابد من التفكير من إيجاد وسائل حفظ لتلك البيانات المرسلة من خلال بناء منظومة أمنية تستخدم احد أنظمة التشفير المعقدة حيث تم اختيار نظام التشفير الانسيابي (Stream Cipher) لغرض تشفير النصوص الواضحة قبل الإرسال عبر الأثير و بذلك امتلكت هذه المنظومة درجة تعقيد عالية يمكن من خلالها إرسال إي بيانات يتم تبادلها ضمن الرقعة الجغرافية آخذين بنظر الاعتبار قدرة وصول الإشارة إلى المكان المطلوب من خلال وجود عدد من البدائل لغرض تقوية الإشارة و الوصول إلى مكان ابعد. حيث تجهز هذه المنظومة للجهات المرسلة و المستلمة حيث تم بناء وسيلة تخاطب (Protocol) لكلا الطرفين لكي تمكن مرسل البيانات من تشفيرها و كذلك تمكن مستلم تلك البيانات المشفرة من حلها بطريقة سهلة دون بذل كثير من الجهد.



## الكلمات المفتاحية

تقنيات البلوتوث، الحكومة الالكترونية، خوارزمية التشفير، خوارزمية حل المشفر، النص المشفر، النص الواضح، المسجل الزاحف، المفتاح الاساسي.


## 1. Introduction:

Origin of the idea of Bluetooth came for the purpose of exchanging information between a number of different devices without the need for wires that transport process is global synthesis wirelessly and especially in linking portable devices such as computers and audio devices where information is exchanged between those devices that have been provided with Bluetooth as described in the figure(1) below.

Figure(1)

And thus was able to this technique over many difficulties experienced by the devices connected wirelessly including the number of wiring and connection type used between devices as well as the type of data that is exchanged between devices. Accordingly knows

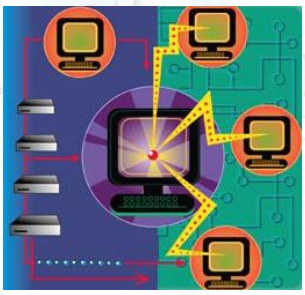
Bluetooth as a communications protocol used radio waves and short covering a limited area depends on the Nature devices sent and received, and this technique consumes little energy, where work is continuing by many scientific centers for the purpose of development of this technology and make it covers the largest area in addition to the inclusion of this technology are many devices such as computers and smart mobile phones and audio devices and visual in order to be exchange of information and data from wires or cables or interference by its users [1].

## 1-1 Reason's for the emergence of the idea of Bluetooth

Given the existence of problems in the wireless communication between devices and operating in an environment close to each other such as using light rays frequency less than the frequency of red light and called infrared and used this frequency in many applications and the most important of remote control devices and called In fared Data Associations and also used in many computer terminals, but these applications and other applications, has suffered many problems, including:

1 - The infrared how vision works and the remote control should be directed directly to the desired device operation

2 - The devices that use infrared works between two devices only, or between the controller and the desired device operation and this so-called one to one and cannot be for more than two that are working in the same or controller can run more than device as described in the figure(2) below.



Figure(2)

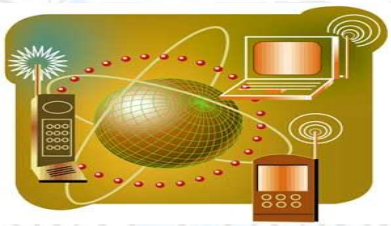
Because of the existence of such problems continued research centers and international companies search for alternatives to overcome such problems which enabled it to create a new technique for the exchange of information between more than two terms dubbed this technology Bluetooth and is a technique with special specifications are installed on a small plate (Radio Module) is installed in the hardware required exchange of information among them wirelessly and thus launched on such devices supported by technology Bluetooth-free wiring as well as it facilitated the operation, where you can all devices nearby in a patch specific to exchange information without any user intervention except operation that Bluetooth technology operates in accordance with the protocol prepared for this purpose[2].

## 1-2 patterns Bluetooth

There are several modes of Bluetooth and a featured these patterns can be summarized as follows:

1.Advanced Audio deployment pattern
2.Style remote control sound and Video
3.Basic Control Style Pictures
4.Publishing year pattern of sound and image
5.Devices pattern of human interaction
6.Pattern of access to the local network
7.Personal network pattern
8.Pattern to access the phone book
9.Deployment pattern Video
10.Style directory service distributor

One pattern described in the figure(3) below [3].



Figure(3)

## 1-3 Mechanism Bluetooth

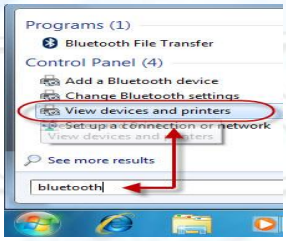
Bluetooth device technology based on the idea of generating radio waves at a frequency of 2,24 GHz, according the International Convention for the use of industrial devices were mentioned where frequency identification cannot be happening any interference during the process of communication that each device has its own frequency and has its own times where technology is used frequency hopping is nice publication where this device to change the value of frequency 1600 times per second and so we do not find any two devices operating under the same frequency and so if two devices are within close geographical area, these devices can establish personal network among themselves as carrying out together change frequency one way and one time to avoid interference with other personal networks may be present within the same geographical area.

## 1-4 -Verification of Bluetooth

The first thing you should do before you start the Bluetooth connection to make sure that Bluetooth enabled Windows 7 has drivers dongles most Bluetooth and built-in appliances, but if were not able to find any drivers suitable for it, you must install one of the specialized programs in this area. At first you will see the Bluetooth icon in the system tray or notification area, which means that Bluetooth is active (enabled) as described in the figure(4) below .

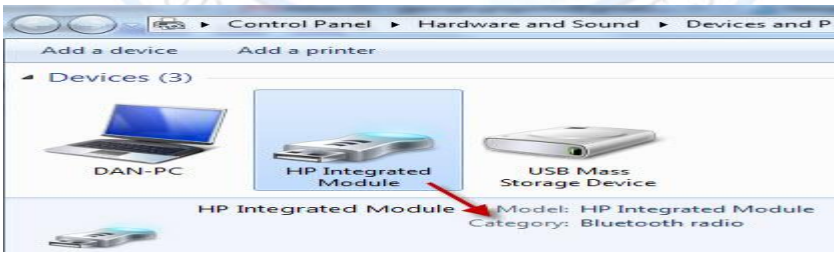

figure(4)

If you are not active you must activate it now, and if you need to make sure that Bluetooth is working correctly as described in the figure(5) below.
Type in the search box on the Start menu Bluetooth word and then click on View devices and printers, and then wait for the search result.




figure(5)

In the new window you will see a list of all devices and printers that are connected to your computer as described in the figure(6) below. Whether the device has a yellow exclamation mark Bluetooth, it means that there is a problem which otherwise it means that the device is working properly.




Figure(6)

If the device has problems, select it, then click explore from the top menu. Follow the wizard's instructions and you will find a solution to this problem[4].


Figure(7)

## 1-5 - Piconet network

Special mesh technology as Bluetooth devices with Bluetooth technology have the ability to recognize what is required of them without user intervention. The fact that segments of the technology has been programmed where they can communicate with each other for the purpose of data transfer, for example, e-mail between mobile phones and computers or control device Stereo with Headphones where these devices creates networking small between devices and accessories called network personal Area Network (PAN) or the so-called its common piconet name. As each network has formed its own frequency and segments are provided with Bluetooth addresses of its own within each department and in the light of those titles are process to connect to a network composed called piconet. Where you cannot get any overlap between the networks that each network frequency differs from other network frequency[5].

## 1-6 The concept of e-government

This is the concept of the most prominent concepts introduced by the information revolution and the Internet, which emerged as a result of technical developments interacting with humans at the level of broad geographic and objective basis for this concept is to make all government departments to integrate with each other and provide services and between the citizens and the private sector directly and electronically [6]. Realized the importance of e-government through the realization of the fact that today's world became a judge at an advanced society as there are three basic conditions are transparency, accountability and good governance [7]. E-government suffers many of today's problems, including unemployment, poor security aspects, the negative impact on employment rates, high cost for the construction of electronic data, and the fear of limiting the work of e-government on a specific category of people[8]. With the developments of government services e-government offers many benefits including raising the level of performance, increase data accuracy, reduce administrative procedures, the optimal use of human energies[9]. E-government has passed several stages including, staff training and rehabilitation, providing the infrastructure for e-government, documenting the old paper-based transactions, and programming of the most common transactions[10]. Finally, the construction of e-government powerful must provide a number of requirements, including providing research environment through the provision of communications systems effective for the transfer of data to and from governmental institutions and individuals, the community and this is located on the communication networks in addition to providing computer with high efficiency for the purpose of the success of the work of the e-government [11].

## 2 - Bluetooth applications

1 - connect mobile devices with each other within the geographical area and also connected with microphones or devices with audio devices.
2 - Use this application with attached parts as input and output devices without the need for wires between the computer and accessories.
3 - possible to use this application to build network computers within the geographical area where the files are transferred with each other across platforms prepared for this purpose (transportation system elements)[12].

## 2.1 Features Bluetooth

1-Wireless Technology Bluetooth feature Severity and low capacity in addition to a few cost.
2- feature this technology offers a variety of services through which enables communication between devices and exchange data between them.
3 - Bluetooth is a sender and recipient and representative protocol stack

## 2.2 Bluetooth security

The security situation for Bluetooth either be unsafe or a certain level of security locks before sending or his level of security actor has been taking into account four factors include security this technique:
1 - We need the reliability of 128-bit random for the purpose of ensuring the reliability of this device.

2 - Length of the encryption key from 8-bit to 128-bit is used for encryption purposes.

3 - The Bluetooth device select my address component number of 128-bit.
4 - Bluetooth address of the 48-bit component where each device individually numbered defined by the Association of Electrical and Electronics Engineers (IEEE)[12].

## 2-3 Main problems that have been solved by using Bluetooth

1 - The means of communication between the devices are wireless means making it easier to move devices from one place to another and without any effort.
2 - Bluetooth device technology is less cost as compared with other communication devices where this technique was manufactured in the form of card or in the form of computer Dongle placed at the entrance or USB comes integrated in the mobile or any electronic piece is useful for mobiles and data transfer between devices
3 - Bluetooth differs from techniques other wireless devices that those devices rely on the concept of connection to another device that is those devices opposite and close and on a

single line as is the case in remote control systems and that use infrared and which must be Dimension limited IE within range of vision and mobility reference to only one device one to one as well as the protocols manufacturer (Line Of Sight) for each company differs from protocol factory in another company and this disagreement to the case in Bluetooth surpassing such problems [13].

## 2-4 Overcome obstacles jamming problems

It is known that the exchange of information between devices using radio signals GH 2,45 frequency may occur many overlaps between these frequencies, leading to a phenomenon of confusion and this is what we see in television sets. The Bluetooth technology has solved the problem of jamming the fact that Bluetooth signal is weak and the amount of 1 million watts and is very small if compared with other devices and signals measured by sodomy and not parts of a watt. The weakness of this reference make it able to penetrate the walls of offices and facilitate the circulation of information and control between these isolated offices. The frequency range allocated for Bluetooth is between (2,40 (GHz 2,48, where it is the process of scanning rate of 1600 times per second as the two devices exchange information with each other and can be used one of the confined frequencies (2.40 to 2.48 GHz) cannot be more than two working on the same frequency and the same time, where is one to choose frequencies at random within the range specified for these frequencies and thus solved Bluetooth problem of overlapping between devices and even if there were, when Seen tremendous amount of hardware in a particular environment, the interference amounting to a fraction of a second one and thus does not affect the exchange of information[14]. .

## 3 -Traded data via Bluetooth technology

It is known that send data via Bluetooth or via any technology to send and receive wireless ensure that the data vulnerable to listen T. them and hence the Bluetooth in mobile phones lead to violation of the privacy of users and steal their data and their addresses telephone, leading some manufacturers to provide these devices concealment programs as there are many blades when you connect any two devices are some of the programs provided in some devices, including data theft via Bluetooth where the attacker can connect to the device without alerting the owner of the device and so steals that device inventory of additional files to steal the phone book and business card and other information and happen this type of attack when the Bluetooth is in the invisible visible as the phone is in visible mode by compatible devices located within the area of communication and allow it to communicate with each other and exchange data between them. There are also other ways of exposure to data stored on the devices supported Bluetooth and including way back door where it can be this way control and use of the device fully by the opponent, but can use the device return by the opponent for the purpose of access to the Internet or to make a connection using certain programs . There are also other ways to access devices contrast by the opponent as called this method bluebag where built this way to create a serial connection of the device which can be attacker from using some commands through which control the information and make a connection and send text messages and read short messages and

Many other operations as there is another gap resulting from the loss or the loss of some portable devices, which can be of obtaining such devices make contacts and send messages and impersonate the owner of such devices as well as the exploitation of data those devices supporting Bluetooth technology[15].

## 3-1 Data Protection traded via Bluetooth

1 - Avoid the use of important information in public places when such information is encrypted.
2 - Close Bluetooth when you're working on it.
3 - When the Bluetooth is in the invisible visible must convert to the situation off.
4 - Delete the existing hardware in the list of paired devices.
5 - Run protective devices Bluetooth[14].

## 3.2 Data encryption protocol plain-text

To maintain the security data traded, whether that data sent or received via Bluetooth to be encrypting the data to avoid cases objection that may occur during traded between devices and single out the data transmitted between computers that those encrypted data need returned to the pre-encryption and this requires encryption protocol is based on the encryption algorithm and solution algorithm for encrypted data that have been received [15].

Before starting the preparation of encryption protocol must specify the encryption system used was chosen as one of the encryption systems with a high degree of complexity of the code is difficult for analysts to find the key to the solution, the system chosen is a stream cipher system . A stream cipher denotes the process of encryption where binary plaintext is encrypted one b. The encryption process can be expressed as :it at a time. The simplest and most often used stream cipher for encrypting binary plaintext is where the bit at time interval t of a pseudo random sequence k(t), is combined using modulo two addition with plaintext bit, p(t), at time interval t to produce the cipher text bit a time interval t, denoted by c(t). The sequence k(t) is called key stream for the stream cipher. The encryption process can be expressed as: $C(t)=P(t) \oplus K(t)$ , where $\oplus$ denotes modulo two addition. The decryption process can be expressed as: $P(t)=C(t) \oplus K(t)$ [16]. Encryption protocol includes the construction of an encryption algorithm includes the following steps:

### 1 - Basic key

Is among the symbols or letters shall preferably be non-current sentences that these symbols is the encryption key and the key to the solution and supports a number of those symbols to creeping along the Registrar who fed binary bits representation of those symbols.

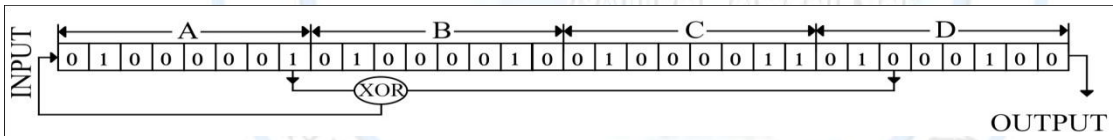
## 2 - Shift register

The main component of most stream cipher is shift register (SR). The general structure of SRs is consist of m stages; each stage can hold one bit. A clock input, on every pulse of the clock controls the SR; the bits are shifted one stage to the right the bits, which generated at stage 0, form the output of the SR. As the bits are shifted to the right, it is necessary to supply new bits to stage m-1 for the SR of length m. These bits can be obtained from a feedback loop, containing a modulo which calculates the value of the new bit SR with feedback called feedback shift register (FSR) [17].

## 3.3 Data decryption protocol cipher-text

Is the same encryption protocol and includes the following:
1-The primary key Basic Key: The key must be known by the basic entity received.
2 - Recorders creeping: and specifications must be fed a primary key and when it comes cipher text to the recipient and which analyzes the process of analysis, where are the same procedures that have been in the process of encryption and so on the opposite case is clear text.
Encryption protocol and protocol analysis is one follows the same steps as those message and received him [18] .

The following diagram represents creepy recorder was fed an essential key is ABCD



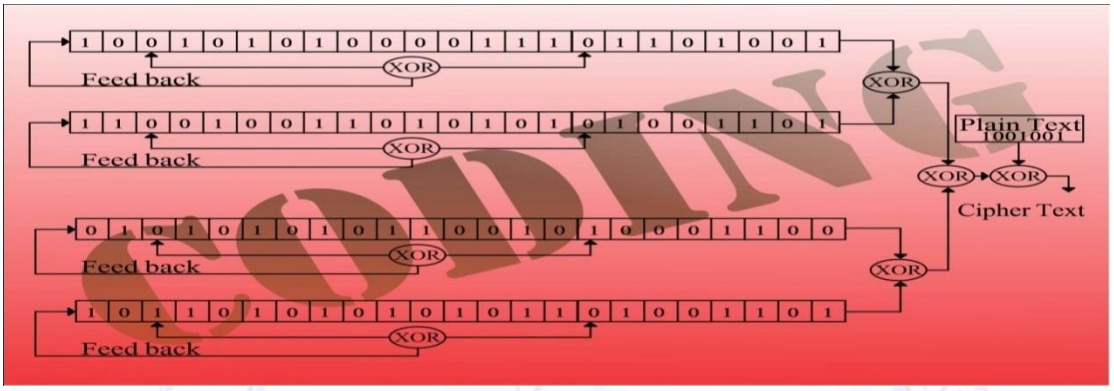

| Encrypted bit | shift registered bit | | plain text bit |
|---|---|---|---|
| 0 | 0 | XOR | 0 |
| 0 | 1 | XOR | 1 |
| 1 | 0 | XO R | 1 |
| 0 | 0 | XO R | 0 |
| 0 | 0 | XOR | 0 |
| 0 | 0 | XOR | 0 |
| 1 | 0 | XO R | 1 |
| 0 | 0 | XO R | 0 |

Table(1)

## 3-4 Encryption and analysis system

Encryption system was used flowchart Stream Cipher where the encryption system is built of four shift register then connect all two shift registered together where they are collected (XOR) abroad bit of SR1 registered with abroad bit the outside of the second registered SR2 then this bit is collected (XOR) with abroad bit the outside of the output of the collection

(XOR) registered SR3 and SR4 and so we get a final bit encryption is collected (XOR) with the clear-text bit to get a bit cipher text as described in the figure(8) below. Where they are taking into account the lengths recorders creeping and method of collecting the number of cells to get a bit of nutrition for registered creeping also been taken into account feed all registered creepy key primary, taking into account to avoid the length of a repeat of the deciding one to ensure random prevent the repetition of the primary key of the same or part of that key and thus guarantee higher degree of complexity is difficult for the analyst to find the encryption key when analyzing encrypted texts that can be obtained during the transmission process or access to places of storage of such data after the current development in Bluetooth technology.

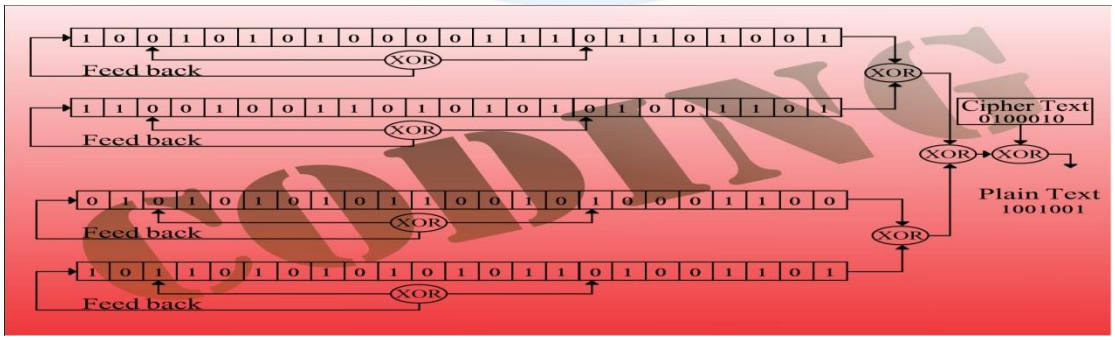



Figure(8)

I have been taken into account the length of each registered creepy and preferably have a length of recorded creeping one setup state and was also taking into account the symbols used in the primary key for a state of balance between the number of bits (1) and the number of bits of the type (0) for the purpose of obtaining frequencies close lead to increased complexity out of every bit creepy recorder.

## 3.5-The encrypted text analysis system

recipient is equipped with encrypted messages to the same primary keys that were used in the encryption process well as creeping recorders and method of linking them together is the same as that used in the encryption as described in the figure(9) below.




Figure(9)

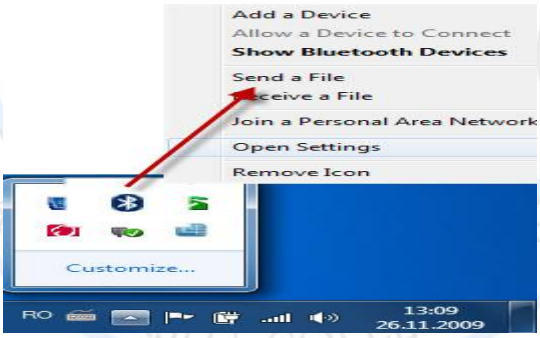
And after that has encryption process text has been used Bluetooth technology to send encrypted data and the same encryption algorithm and then solve the clear text by the party that received the message and thus enable us to ensure that data is securely even if enables anyone to get that information encrypted it difficult to analyze and get the clear text because of its encryption systems, aerodynamics of high degrees of complexity is difficult for the analyst of code analysis and to obtain clear text and hence the recipient of encrypted messages to close before the implementation of Bluetooth analysis algorithm for fear of rags that occur using the technique Bluetooth.

## 3-6 Way send and receive files

After becoming the files ready to send and receipt where undergone those files and according to their importance for some security controls, including file encryption task and the fact that ready those files must be a hardware stored on them that data contain an operating system talk and not a Windows system (7), as this system has the ability to send and receive data being known as Bluetooth hardware requirement to be dealing with this software contains Bluetooth technology, where it is the process of sending files according to the following steps :

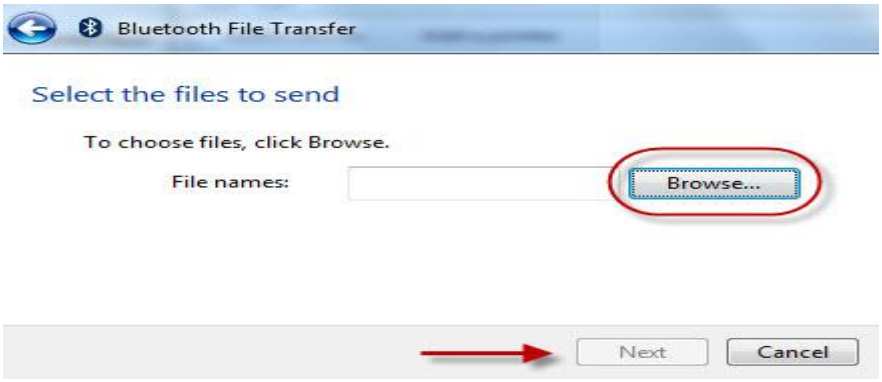
1 - Make sure Bluetooth enabled and if you do not do open it. .

2 - Through the system tray or notification area can see the Bluetooth icon If the Bluetooth symbol Green This means that the Bluetooth enabled file and select Send or search for Bluetooth in the search list in the box and click operation began transferring files and select Send file as described in the figure(10) below



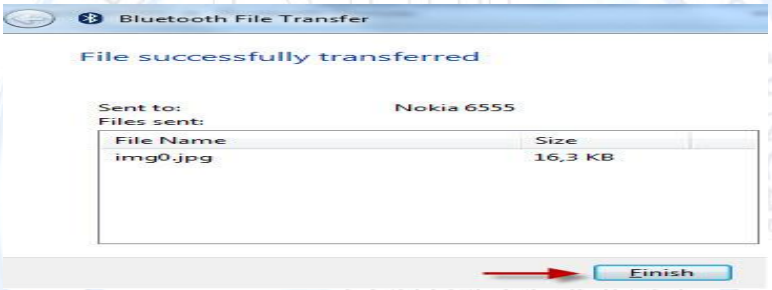

Figure(10)

Select the device you want to send the file and click Next and then click Browse to select the file you want to send and then Next, as shown in the figure(11) below




Figure(11)

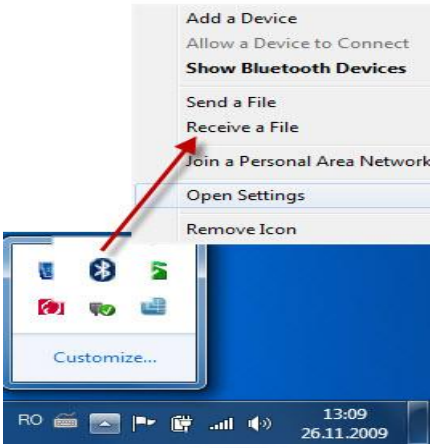
A new window will appear see through review of the transferred file, and then click Finish to exit
out of the window as described in the figure(12) below




Figure(12)

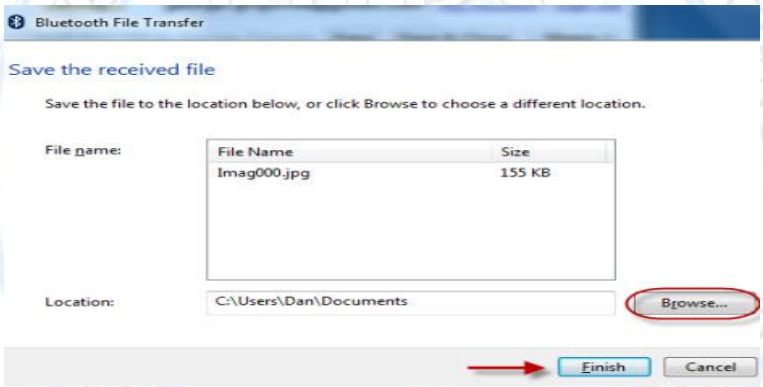
## 3-7 The process of receiving files

Search for Bluetooth in the search list in the start box and click on the Bluetooth file transfer. Then select a file to receive wait until you select a file on your computer as described in the figure(13) below




Figure(13)

Select the file to be sent to the computer through a Bluetooth connection, wait until he finds the computer, select it, and in the next window you will see the name and the size of the file and you choose a place to save it. Click on Browse to choose one location different than the default, and then click Finish as described in the figure(14) below




Figure(14)

Now the file is received and stored in a location that is specified by the recipient.

## 4.Conclusions and recommendations

1 - The data that is sent to beneficiaries using this technique with a few quick cost of trading.
2 - Using algorithms to encrypt critical data in Bluetooth technology to become one of the means easy application in e-government.
3 - Use Bluetooth in electronic government service facilitates the trading of e-mail and in particular circulars, books, required to answer them and that are traded in many institutions that use this kind of applications.
4 -The pros use Bluetooth technology after securing is easy access to all sides and only send one regardless of the reach of the fact that these data seen it who has the keys to the solution.
5 -The disadvantages of this technique, which was deduced from the application that the distance of sending data with this technology is limited where they can solve this problem by re-send those texts by terminals that receive such data by providing those terminals programs transmission without interference from the user of that terminal.

6 - We recommend the development of this technology because of its great importance by providing networks that use this type of application to develop reference to devices up to the largest possible distance to ensure access to data sent to users in organizations that use this kind of applications.

## References

1.Bluetooth sig. retrieved , "how Bluetooth technology works",2009

.2."Palowireless ;Bluetooth Resource center",2011

3."IRDA versus Bluetooth; A complementary comparison",2010

4."Study; Bluetooth Development outpacing",2008

5.http:// forum. Scriptat.com/showthread.php?t=2128

6. Alaa Abdul Al_ Razak Salmi, "electronic administration",Amman, Dar Wael, 2008

7.Sahar Kaddouri Al_ Rifai," e-government and how to apply",2011, is available in http://www.univ-chlef.dz

8. Ali Mohammed Abdulaziz," e-government applications",2012, available at http://www.verypdf.com

9.Wajib Gharibi ," e-government concept, requirements, benefits", 2009, available at http://islamfin.go-forma.net

10." Stages of the transition to e-government", available at www.alriyadh.com

11. Diala Jammil Al_ Rizzi," e-government and constraints applied", 2012, available at: http://umco.maktoob-blog.com

12.Helsinki University of technology retrieved," Bluetooth security", 2009

13.http://what-is-what.com/what_is/wibree.html

14.http://Coeia.edu/index.php/ar/asuurance-awarness/articles/45-wireless-security/338-bluetooth.html

15.Matusi M and Yamagishi A.," A New Method for Known Plaintext Attack of FEAL Cipher",EUROCRYPT 1992.

16.Menezes A. and Van A. J. and Vanstone S.A., "Handbook of Applied Cryptography", CRC, Press, 1996.

17.Schneier B., "Applied Cryptography, Protocols, Algorithm, and Source Code, C Language", John Wily and Sons, Inc ,U.S.A, 1996.

18.Biham E , and Shamir A., "Differential Cryptanalysis of the Data Encryption Standard",Spring Verlag, 1993.