Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/18227
DOI URL: http://dx.doi.org/10.21474/IJAR01/18227

RESEARCH ARTICLE

REVIEW PAPER-TRENDS IN PAIRING IN WIRELESS TECHNOLOGY

Chetan Navnitrai Dave[1] and Dr. Mallika Ravi[2]

1. Asst. Professor, V.S. Patel College Of Arts & Science, BCA-BBA Course, Affiliated to Veer Narmad South Gujarat University Surat Gujarat India.
2. Assitant Professor, S.S.Agarwal College, BCA course, Navsari, Affiliated to Veer Narmad South Gujarat University Surat Gujarat India.

Manuscript Info

Manuscript History
Received: 19 November 2023
Final Accepted: 29 December 2023
Published: January 2024

Key words:-
SSP, Pairing, MITM, Bluetooth, IOT

Abstract

Pairing research has been conducted since the invention of Bluetooth. Today, tethering is also used in IOT. Bonding has a lot to do with security. The global IoT market size will grow from USD 399.41 billion in 2022 to USD 486.7 billion in 2023 at a compound growth rate (CAGR) of 21.9%. The IoT market in India is projected to reach $27.31 billion in revenue by 2023. Industrial IoT dominates the market and is projected to reach a market size of USD 9.67 billion by 2023. Revenues are expected to grow at a compound annual growth rate (CAGR 2023-2028) of 17.05%. The global Bluetooth 5 market exceeded USD 4.1 billion in 2022 and is projected to grow at a CAGR of 11.0% during the forecast period 2022-2027 to reach more than USD 7.0 billion by 2027. The India wireless speaker market is expected to reach USD 271.32 million in 2023 and will grow at a CAGR of 21.20% to reach $709.56 million by 2028. In short, growth projections are quite high, so security considerations are very important. I looked at 100 papers in this review and categorized them below.

11 papers on attacks
8 papers on security against attacks
32 papers on new algorithms, new architectures and systems
14 papers on evaluation of the current connection method. Their components
15 papers on proposals for existing coupling techniques,
20 papers on existing coupling techniques.

Objectives of this review are study of how an attack can be simulated on pairing and how to simulate defensive mechanisms.

Introduction:-

Development of short-range radio technology, later known as Bluetooth, was started in 1989 by Nils Rydbeck, CTO of Ericsson Mobile in Lund, Sweden. The aim was to develop wireless headphones according to Johan Ullman's two inventions, SE 8902098-6 published on 12-06-1989 and SE 9202239 published on 24-07-1992. Nils Rydbeck provided specification to Tord Wingren and development to Dutchmen Jaap Haartsen and Sven Mattisson. Both worked at Ericsson in Lund. The main design and development started in 1994, and by 1997 the team had a working

Corresponding Author:- Chetan Navnitrai Dave
Address:- Asst. Professor, V.S. Patel College Of Arts & Science, BCA-BBA Course, Affiliated to Veer Narmad South Gujarat University Surat Gujarat India.

solution. From 1997, Örjan Johansson became the project manager and promoted the technology and standardization. In 1997, Nils Rydbeck was contacted by Adalio Sanchez, who was then head of RandD, an IBM ThinkPad product. Collaboration to integrate a mobile phone into a ThinkPad laptop. Two engineers from Ericsson and IBM investigated the idea. The conclusion was that the energy consumption of mobile phone technology at the time was too high to integrate it into a laptop and still achieve sufficient battery life. Instead, the companies agreed to integrate Ericsson's Short Link technology into both the ThinkPad laptop and the Ericsson phone to achieve the goal. Since neither IBM ThinkPad laptops nor Ericsson phones were market leaders at the time, Adalio Sanchez and Nils Rydbeck agreed to make short-link technology an open industry standard to allow each player having maximum access to the market. Ericsson was involved in short circuit radio technology and IBM patented the logic layer. Adalio Sanchez of IBM then recruited Stephen Nachtsheim of Intel to join, and Intel later also recruited engineers from Toshiba and Nokia. In May 1998, the Bluetooth SIG was launched with IBM and Ericsson as founding members and a total of five members: Ericsson, Intel, Nokia, Toshiba and IBM.

What is Bluetooth pairing?

Bluetooth pairing is a form of data logging for connecting devices. By registering device information (pairing) between devices, they can establish a connection. To use a Bluetooth device, you must first pair it with another Bluetooth device. Pairing is a bit like exchanging phone numbers. Just like you have to exchange phone numbers with the person you want to call, connecting Bluetooth devices requires them to be paired first to record each device's pairing information. If the device is paired for the first time, there is no need to repeat the pairing process. This is because every device has the necessary information stored on it and therefore can be connected easily.

The pairing process SSP facilitates pairing of Bluetooth devices. The remaining paper is divided into 6 sections as follow.

1) Survey that took place for pairing
2) Attacks on pairing
3) Safety against pairing attacks
4) Evaluations of existing pairing protocols
5) Suggestions for existing pairing methods
6) New Approaches for pairing

Survey

A usability analysis of secure pairing methods taken place in 2007. Users clearly distinguished between the methods, but at that time SSP (Secure Simple Pairing) was not launched. [99] A safety study was done. They described a variety of different commonly used countermeasures. Since then, many other security attacks and many other countermeasures have been proposed. They used the human factor in the BEDA protocol. They emphasized the need for a longer and more complex plaque. Many proposals to change the 6-digit pairing key have been theirs so far, but none have been accepted by the Bluetooth Special Interest Group (SIG). [97]

A study on research mechanisms taken place. They identified and described various research questions and challenges in the field of wireless communication. [91]

Evaluation of Bluetooth security threats and solutions taken place. They gave an overview of the biggest attacks that Bluetooth has faced over the years, as well as some possible solutions. A typical study, such studies should be done regularly. [82]

Analysis of the security risks of Bluetooth devices, listed various attack types and advised the user to be vigilant when using Bluetooth. [84]

An offer was made for future transformative applications of Bluetooth technology. He listed some promising future Bluetooth applications and hinted at possible future Bluetooth research. Bluetooth is here to stay. right? [58]

They deployed more advanced Bluetooth stacks in hosts, which is a more interesting and profitable target for attackers. Additionally, Bluetooth devices that have more features or are designed outside the Bluetooth definition (such as smart locks) tend to have security issues. SSP or Enhanced SSP should not only be for Bluetooth, but for all devices that require pairing. [55]

The (ECDSA) Electronic Digital Signature (EDS) has eliminated most of the problems associated with signing a paper document. Why was manual signature not replaced by ECDSA? [37]

A Modern Study of Bluetooth Wireless Technology took place. Their article was intended as a brief introduction to the many challenges that Bluetooth technology faces if it is to succeed as an adhoc networking technology. The work done in this area is presented . [28]

They explored Bluetooth security solutions. Their article provides an overview of the main attacks that Bluetooth has faced over the years and some possible solutions were discussed. Such surveys should be conducted at regular intervals[31].

A comprehensive study on digital signatures took place in 2021. There article provides comprehensive information about the digital token and its benefits.[22]

A Bluetooth Low Energy security and privacy study took place. Considering all the described security holes and attacks, designing a secure BLE device can seem very difficult. As they showed, the Bluetooth SIG addressed most of the threats and suggested ways to mitigate them. Therefore, building a secure BLE device can mostly be achieved by using all the protections provided in the specification in its latest version. [16]

A study on security analysis of non-radio pairing protocols had taken place. They proposed a new out-group classification by evaluating several security guarantees such as confidentiality, data freshness, integrity, data authenticity, liveness and channel availability. [12]

A research on Elliptic Curve Cryptography based secure healthcare system communication with mobile devices took place. This survey discusses various technologies that include mobile healthcare, wearable sensors, secure key distribution, group key management, health monitoring, etc. [8]

A literature review on Bluetooth security threats and mitigations was conducted.. They conducted a systematic literature review of articles published in ACM and IEEEXplore. Their detailed analysis compiled a list of 48 academic papers that focused on an overview of Bluetooth functionality, threats and mitigations studied by previous researchers. Their findings show that there are a number of Bluetooth attacks that can lead to the loss and exploitation of user data. The purpose of this article was to inform users about relevant attacks and provide them with useful ways to mitigate them by analyzing previous research. [20]

An information security and privacy threats caused by Bluetooth low energy in IoT and mobile devices were investigated. In this study, they critically analyzed the BLE security protocol and identified security flaws in device pairing that lead to many security and privacy issues. They then present a comprehensive taxonomy of different attack vectors, focusing in detail on the different techniques for each threat, and provide recommendations to mitigate those threats. They provided some recent attack summaries and introduced some popular tools for analyzing, pinpointing and mitigating vulnerabilities. Finally, they discussed the new features and potential new application areas that will drive the adoption of BLE in future IoT devices. [21]

An overview of additions and changes to the RSA algorithm was presented. All techniques are useful for speeding up the RSA algorithm and improving security. Each technology is unique and can be used for different applications. [3]

A study was conducted on eavesdropping in Bluetooth networks. They expressed the security flows of Bluetooth networks, described how eavesdropping can happen. [6]

A paper was presented on elliptic curve cryptographic analysis. its applications - challenges - recent advances and future trends - EC is used to secure open communication channels and make the digital age accessible to authenticated users.[1]

Change of matrix function keys were implemented.. They proposed a key exchange protocol similar to the classical Diffie-Hellman protocol based on the semi direct product of two cyclic semi group matrices over _p. One of the

semi groups is additive and the other iterative. Their protocol never exposes the ability of any matrix or element of _p, so all standard attacks against protocols like Diffie-Hellman are not usable. [11]

Attacks

M Thrinatha Reddy, Et.all- in 2011- gave an overview of Man-in-the-middle Attack and Countermeasures in Bluetooth Secure Simple Pairing. They tried to solve the man-in-the-middle problem by storing the keys in a database. They also recommended using encryption before starting the pairing. [88]

A Man-in-the-Middle Attack Against Bluetooth Secure Simple Pairing took place, The attacks were based on falsifying the data sent when exchanging I/O functions and also that the security of the protocol is likely to be limited by the least effective or least protected device type characteristics. The less secure device and the more secure device can be decrypted using an optimal algorithm. [86]

They launched a new Bluetooth Man-In-The-Middle Attack Based SSP using OOB association model. SSP association patterns such as Numeric Comparison, Jobs Only and Password Entry have been proven in the literature to be insecure. It is necessary to study how to eliminate their weaknesses. [74]

A man-in-the-middle analysis in SSL attack was performed. They implemented ARP poisoning and fake certificate attack (phishing attack). Can such an attack happen to SSP? This should be investigated. [79]

The t-mobile made a "man-in-the-middle attack" against Wi-Fi calls was implemented. They used ARP spoofing, DNS cache poisoning to attack. Can such an attack be made against SSP? This should be investigated. [64]

The Bluetooth pin was broken again; they broke their Bluetooth pin and used a more secure algorithm. Well, this 6 digit number is a week, so it can be broken.[46]

Bluetooth Low Energy passkey authentication, the Passkey Entry assembly method of the Bluetooth Low Energy communication standard cannot guarantee the authentication of the respondent to the author even with a one-time PIN, proven. The passkey injection method provides protection against active man-in-the-mid (MITM) attacks, because an active man-in-the-mid will succeed with probability 0.000001 for each method. Many attacks have been made against SSP. [49]

The Bluetooth PIN code was broken, they organized an attack against the Bluetooth security mechanism. Their results show that using algebraic optimizations, the most common Bluetooth PIN code can be cracked in less than 0.06-0.3 seconds. If two Bluetooth devices are paired in a hostile area, they are vulnerable to this attack. SSP is not completely secure, that has been proven many times. [50] an algorithm was created to perform the ET.ALL attack and showed how the first test used by the attacker limits it. They provided a model that should be practically tested in all environments.[47]

A method obfuscation attack against Bluetooth pairing took place... They introduced a new attack against BLE pairing in BT version 5.2. The attack uses what they call Method Confusion to get the MITM status between two paired Bluetooth devices. It exploits a critical design flaw that was acknowledged by the Bluetooth SIG after their disclosure.[30]

An organized attack against Bluetooth was implemented. They present Black tooth attack against Bluetooth BR/EDR. Their attack exploits several security holes in the Bluetooth configuration. If you want to personalize a Bluetooth peripheral, connect to the victim's device (such as a Smartphone) and extend access rights by changing profiles. As a result, an attacker can issue arbitrary commands and steal sensitive data from the victim's device without warning the user or interacting with the user during the entire connection key authentication process, without a malicious agent pre-installed on the victim device, and without knowledge or authentication of connection key [17]

Safety Against Attacks

A researched took place on pure pairing of audio devices with human help. They converted cryptographic data into a verifiable human voice. But at that time there were also stupid Bluetooth devices for which this method is not

suitable. IN 2009, they offered secure pairing for devices with limited interfaces. They used the human factor in the BEDA protocol. [98]

Man-in-the-Middle Attack and Countermeasures were studied in Bluetooth Secure Simple Pairing - MITM attack on PHY layer can be avoided by using anti-jamming technique in SSP model. A MITM attack on the PHY layer can be avoided by using anti-blowing techniques in the SSP model. Anti-bullying technologies are not available everywhere. [85]

Bluetooth security review was conducted. A number of possible countermeasures against the attacks are proposed. Research into comprehensive countermeasures is an ongoing process. [70]

They proposed security measures against man-in-the-middle attack in key exchange. They proposed double encryption using the public key of both parties and found a way to achieve protection even if an attacker decrypts the public key. The proposed solution should be tested. [78]

They proposed a defense against MIDA ATTACKS. Secure simple pairing; they proposed a solution for MITM attacks. They proposed a solution for MITM attacks. Their proposal was A cryptographic solution to start before SSP. that should be tested in practice. [83]

An analysis of the MITM attack in Secure Simple Binding took place. An algorithm that detects a MITM attack has been presented. The proposed algorithm should be tested in practice.[62]

Compromise of one network does not lead to compromise of all networks and each sensor network has its own as (authentication server). Each sensor network has a private key generator (PKG) that is part of the authentication server AS. Let SKPKG be the private key PKG of the sensor network and PKPKG be its public key. Here, it is assumed that an intruder can attack only with a Smartphone. If one Bluetooth device is attacked, Piconet should investigate how it affects other devices.[60]

Once an attacker has compromised the gateway node, the entire IoT system can be down and become critical. To solve this, they proposed that a new client node could become a member by generating a cryptographically signed authenticator. The identity of the token (client) is controlled by the administrative node. This concept can be used in a piconet. The main device can play an important role. [41]

Evaluation

A tool to analyze device pairing methods was developed. and tested 4 different pairing methods. After that came many other bonding methods. Can a generic tool be developed to test all binding methods? [94]

A comparative study on secure device pairing methods took place. The results show that simple number comparison is generally quite attractive, fast and safe and easily accepted by users. [96]

Evaluation of the security aspect of different WEP protocols took place. Now wpa2 exists, but different binding methods should be evaluated. [73]

The security of WPE and WPA was tested, now wpa-2 is in practice and was also attacked.[76]

A study on Wireless Ad-Hoc Network Attacks and Routing Protocol Attacks was performed. They looked at security threats in mobile adhoc networks. It is necessary to investigate whether there are such dangers in short-distance networks. [80]

A study was performed on wireless Ad-Hoc network attacks and routing protocol attacks. Are such attacks possible through SSP? This should be investigated. [75]

A proposal was made for internet protocol security for spoofing attacks. They explained how VoIP works and what its weaknesses are?. Whether spoofing attacks are possible in SSP needs to be investigated. [77]

How Diffie-Hellman fails in practice was shown. Diffie-Hellman key exchange is a cornerstone of applied cryptography because in practice it is often less secured than commonly believed. Diffie-Hellman key exchange is only part of any protocol. It is not synonymous with protocol. [48]

The security analysis of mobile phone Bluetooth transmission was done and improvements to the link connection mechanism were suggested. The link connection mechanism of the link layer was analyzed, 3 different secure data transfer modes were discussed. It was mainly about the process of matching two mobile Bluetooth devices in the third safe mode, and the security of data transmission could also be ensured, which at least partially compensated for the hidden problems of the underlying Bluetooth protocol. Not only must the data transfer be secure, but also the connection. There are no MULTIPLES. [52]

RSA is strongest and finding a crack of 200 digits requires 4 billion years of computing time! However, this claim is questionable. [39]

Cyber security flaws were analyzed and argued that no algorithm is perfect and can be compromised under certain conditions. [40]

Formal authentication analysis was introduced for pairing Bluetooth devices. They point out that the simple binding protocol specification appears to allow no user input other than confirming that two hashes are the same. In that sense, their symbolic model is an appropriate abstraction of user interaction in a simple binding, and the problem arises with concurrent sessions. Piconet has concurrent sessions. From this perspective, this study is valuable. [51]

A comparison of digital signature algorithms was performed. The difference between EdDSA and ECDSA was presented. The differences are based on several parameters such as key length, signature size and key length. Different digital signatures have been evaluated from different perspectives. Such an analysis can be performed for binding and for secure simple binding.[27]

Theory and application analysis of password-authenticated key exchange was carried out. As knowledge of PAKE protocols continues to evolve, they provided an overview of where they stand after 30 years of research. Why is SSP not evolving? [23]

A weaknesses in existing protocols and settings was highlighted. A security token was offered. In many security algorithms, the token plays an important role. [89]

Suggestions:-

Security measures had been proposed in wired and wireless networks. It was believed that humans played an important role in ensuring wireless security. Today it seems profitable; people play an important role in cyber security! I think algorithms play a big role. [90]

The hopping protocol improvement was proposed, the LEAP protocol was improved to use multiple base stations to minimize data loss, and the proposed solution could also identify the compromised inter-base station. Implementation of this protocol for a piconet (a group of 8 or more Bluetooth devices connected to each other). [71]

A general approach to Bluetooth network security had been offered. They provided a list of combination key (generation) algorithm used for matching. A good paper for those who want to study relationships. [66]

A secure communication architecture was proposed for the Internet of Things using smart phones and universal edge computing in environmental monitoring. They evaluated the performance and security issues of a Bluetooth-based secure simple pairing concept using elliptic curve encryption using various performance metrics such as throughput, end-to-end delay, and packet rate. Elliptic curve cryptography is currently widely used in various cyber security algorithms.[67]

Automating Bluetooth Pairing with Near Field Communication (NFC) was proposed. Showed how to make pairing automatic (unlike Bluetooth mobile where visual confirmation is required). With NFO (nearby found objects) displayed. Can't we replace the visual verification with an automatic pairing mode? [65]

A scalable and secure architecture for distributed IoT systems had been proposed. They stated that False Miner requires previous (n - 1) blocks to mine and a window size of n blocks. The window size is kept secret and only sent to miners with the birth block. [44]

A sliding block architecture for IoT had been proposed. They suggested that an approach based on the SEMIoTICS model provides a holistic approach that includes the security, privacy, reliability and interoperability of IoT/IIoT systems. Security, privacy, reliability and interoperability are all characteristics of strong security, all are characteristics of strong security, all are characteristics of strong security, all are characteristics of strong security, all are characteristics of strong security. [45]

A mathematical analysis was done and adopted Diffie-Hellman Elliptic Curve (ECDH) to encode messages. They also published another paper on the public exchange process of an elliptic curve Diffie-Hellman cryptosystem. They implemented an information security system in restricted areas. The proposed system with rich dynamics, which is confirmed by the software implementing the ECDH key exchange algorithm and decryption algorithm, has been successfully built. [35]

Authentication of IoT terminals based on proximity and dynamic device pairs using a decision tree method. Research results show that authentication-based proximity and dynamic device pairing with a decision tree for IoT devices is better than without a decision tree. Connectivity is also important in IOT, and there is still no universal approach to connecting IOT devices. [53]

Elliptic curve encryption technology with digital signature algorithm was introduced. They provide a complete description of the proposed ECDSMR method for creating and verifying an electronic digital signature using elliptic curves. The proposed electronic digital signature model with message recovery is implemented with the Shnorr signature algorithm, which allows data to be recovered directly from the signature like RSA-type signature systems, and the amount of data to be recovered is variable, i.e. it depends on the signature information message . [26]

Pairing-based Cryptography in Theory and Practice was discussed; they illustrated the strong connection between elliptic curve cryptography and the theory of divisors, as well as how commonly used assumptions are related to pairing. They also discussed several encryption methods based on pairing. [25]

A secure architecture for an IoT healthcare system was proposed. They proposed that the module include block chain infrastructure and cryptographic key management as consensus algorithms. Binding programming Libraries exist but are not yet widely used.[15]

Modification in RSA Algorithm In Network Security was introduced. Some modified methods of RSA algorithms are discussed. As researchers have tried to use the more secure RSA algorithm, the research in this paper shows that new approaches are being developed every day to improve security and speed up the key generation, encryption and decryption process.[14]

An architectural model was proposed for secure IoT instrumentation. They pushed for it. An edge device must be designed to work only when the first software to run is cryptographically signed by a trusted entity (eg, the device vendor) and its signature matches the public root key stored on the device. Special hardware can be used to store encryption keys and verify signatures. Well, can the same approach be adapted for SSP? That's a big question. [59]

New Approaches

The possibility of making financial transactions with near field wireless technology was explored. Well, today it's just a dream. [100] –

A secure pairing of limited interface devices explored. They used the human factor in the BEDA protocol. This highlight the need for longer and more complex stacks, and their research continues.[95]

A study conducted on a wireless home security system using mobile devices. They developed software for mobile devices that integrate everything from image capture, audio recording, wireless communication devices, email and text messaging. Based on such research, many smart homes have been created in recent years. [93]

The problem of attacks against the system was studied. They proposed a new approach to increase the strength of the existing binding mechanism by adding an additional shared secret parameter called au_id. [92]

Secure public key exchange was proposed during Simple Secure Pairing (SSP) against man-in-the-middle attacks. They proposed the Enhanced SSP Architecture (ESSP). Many such changes were made in SSP. [87]

An introduction of a new symmetric encryption algorithm with fast flexible and high security based on key update was proposed. They proposed a block cipher algorithm using S-Box and XOR gate. Such algorithms should be tested in all possible environments. [81]

A zero-knowledge proof for network security management of wireless networks was launched. They proposed a new security model that deals with three major types of active attacks: MITM attack, clone attack and replay attack. Using a 3-round zero data protocol. This protocol should also be evaluated for SSP. [72]

An interesting proposal was made for a simple, convenient and advanced protocol that uses a well-known authentication method by entering the same PIN code on both connected devices as an alternative to checking displayed numbers. This method is inconvenient for some users. Imagine the user entering a Bluetooth PIN instead of confirming! [69]

A lightweight security architecture based on embedded virtualization and trust mechanisms for IoT Edge devices was proposed. They proposed "SDN IoT Security (SIS)" to improve security. Their proposal is to use device attributes such as device type, device certificate, and device manufacturer certificate as a means of identification. Can this technique be implemented in SSP or not? It should be checked. [68]

Literary with synchronization was proposed. Good innovation suggestion, but can we expect users to design to match? Well, a bit difficult part for the users. [63]

An evaluation of the performance and security of a Bluetooth-based secure simple pairing concept using elliptic curve encryption using various performance metrics such as throughput, end-to-end delay, and packet delivery rate. To use ECC in SSP, more such parameters should be evaluated. [61]

An Architectural Design for Bluetooth Network Wireless Authentication Security was presented. They proposed a new architecture for creating pins. Such models require extensive testing before they can be evaluated. [57]

A hybrid pairing protocol was proposed, a hybrid pairing protocol based on Diffie-Hellman key exchange protocol, MD5 and Hummingbird-2. Such combinations of protocols should be tested. [56]

A Bluetooth-enabled robot that uses a Smartphone during a disaster was introduced. Governments should promote such research. The proposed system shows how an Android Smartphone can be used as a remote control for a robot and various embedded technologies using Bluetooth technology. The proposed system also shows how the robot can be used for travel. [54]

An SDN-based secure architecture design and implementation for IoT-Lab was proposed. They used artificial intelligence with block chain to detect IoT attacks. In this way, they claim, the computation required by the block chain is greatly reduced. Using block chain for local network security is an attractive proposition.[43]

An Edge Decentralized Security Architecture for Industrial IoT Applications had been proposed. They proposed to use SDN (Software Defined Network) to overcome the intrusion problem and improve the security of IOT. [42]

The ECDH curve was analyzed and showed much faster shared key generation with lower storage costs, which is very important in most cloud applications where time and memory are important parameters for data sharing. These findings may or may not be associated with SSP.[38]

An alternative to the DHkey algorithm was proposed Compared with the Diffie-Hellman method to create a shared secret, the proposed protocol has the advantage that it requires fewer numbers at the beginning and the key size is unknown. This possibility should also be tested for SSP.[36]

The elliptic curve Diffie-Hellman encryption system in the process of public information exchange was introduced. They implemented an information security system in restricted areas. The proposed system has rich dynamics, which is confirmed by the software implementing the ECDH key exchange algorithm, and the encryption-decryption algorithm has been successfully designed. [34]

A smart mobile communication system with Bluetooth technology was launched. Traditional attendance system tends to be unreliable due to lack of auditing. The proposed framework uses Bluetooth and a one-time password to authenticate employees and record attendance in a systematic and secure manner. Each student is provided with a mobile phone which would be used to automate attendance marking. The use of Bluetooth should be promoted in this way. And for that, its security must be strong.[33]

An advanced pass code entry protocol for secure, easy Bluetooth pairing was proposed. They introduced a new advanced password injection protocol that successfully protects Bluetooth devices against passive attacks and MITM attacks by halving the computation and communication costs. So far no one has proposed attacking the ESSP. [32]

An analysis of the Full Human-Machine Passkey Entry AKE protocol was performed. Their findings provide guidance to the user and manufacturer in the SHMmodied Passkey Entry field. Although complete CYBORG security cannot be achieved. [29]

A new digital signature algorithm was introduced and tested. In this work, EDSA is proposed and implemented to ensure secure data storage in the cloud and has also been used to access cloud data. This proposed EDSA is developed according to the elliptic curve square points generated by the updated equation. [24]

Improvisation of the security of the Diffie-Hellman key exchange protocol using RSA encryption was proposed. The paper presents a model that would combine the key generation, encryption and decryption steps of the RSA cryptosystem with the well- known DH key exchange to avoid the latter.[13]

Conclusion:-

Pairing is wide research area and Bluetooth whose connectivity does not depend on internet, but it does not mean it does not have security risk and efforts are consistently on for new attacks and their remedies. There is no fix method of either attack or defense of pairing. Various tools and methodologies can be used for that.

References:-

1- Shamsher Ullahet. all. Elliptic Curve Cryptography; Applications –challenges - recent advances, and future trends-A comprehensive survey.2023, https://doi.org/10.1016/j.cosrev.2022.100530
2- OsmanSaleman dEt.all. Ephemeral Elliptic CurveDiffie-Hellmanto Secure Data Exchange in Internet of Medical Things. 2023, https://doi.org/10.1007/978-3-031-09640-2_1
3- Kalpesh Et.all. Overview of Improvements and Modifications in RSA Algorithm.2023, https://www.researchgate.net/profile/Sam-Mohammad/publication/353971385_Overview_of_Improvements_and_Modifications_in_RSA_Algorithm/links/611c9f731ca20f6f862cd5d6/Overview-of-Improvements-and-Modifications-in-RSA-Algorithm.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
4- Janaka Alawatugoda , Authenticated Key Exchange Protocol in the Standard Model under Weaker Assumptions. 2023,https://www.mdpi.com/2410-387X/7/1/1#:~:text=A%20two%2Dparty%20authenticated%20key,and%20modify%20the%20exchanged%20messages.
5- Mohit Kumar Jangid et.all. Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing. 2023, https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_s119_paper.pdf
6- Maruf Farhan and Dr. Nasr Abosata, Eavesdropping in Bluetooth networks. 2023, https://www.researchgate.net/profile/Maruf-Farhan-Rigan/publication/369663505_Eavesdropping_in_Bluetooth_networks/links/65835d0b6f6e450f198d1080/Eavesdropping-in-Bluetooth-

networks.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
7- Xin Huang 1, et al. Efficient and Secure Pairing Protocol for Devices with Unbalanced Computational Capabilities. 2022, https://www.mdpi.com/2227-7390/10/14/2447/pdf?version=1657786993
8- Pandiaraja Perumal et.al. An analysis of a secure communication for healthcare system using wearable devices based on elliptic curve cryptography. DOI:10.1504/WRSTSD.2022.119327
9- Nguyen Dao et.al. proposing a method to design secure digital signature scheme on the ring structure Zn. 2022, https://isj.vn/index.php/journal_STIS/article/view/194/130
10- Nael Rahman et.al. MAKE: A matrix action key exchange. 2022, https://eprint.iacr.org/2021/116.pdf
11- Funda Ozdemir et.al. Development of Cryptography since Shannon. 2022, https://cetinkayakoc.net/docs/r14.pdf
12- Sameh et.al. Security Analysis of Out-of-Band Device Pairing Protocols: A Survey. 2022, https://doi.org/10.1155/2021/8887472
13- Chiradeep Gupta et.al. Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. 2022, https://iopscience.iop.org/article/10.1088/1742-6596/2161/1/012014/pdf#:~:text=This%20paper%20proposes%20a%20model,effectiveness%20of%20the%20proposed%20model.
14- Abhishek, et.al. A Study On Modified RSA Algorithm In Network Security. 2022, https://www.researchgate.net/profile/Dr-Vandana-2/publication/360241707_A_STUDY_ON_MODIFIED_RSA_ALGORITHM_IN_NETWORK_SECURITY/links/626ab93bd99ac24cc4715ea1/A-STUDY-ON-MODIFIED-RSA-ALGORITHM-IN-NETWORK-SECURITY.pdf
15- Vithya and Arockiam. A Secured Architecture for IoT Healthcare System.2022, http://dx.doi.org/10.1007/978-3-030-24643-3_106
16- Matthias Cäsar et. al.A survey on Bluetooth Low Energy security and privacy.2022, https://doi.org/10.1016/j.comnet.2021.108712
17- Mingrui A et.al, Blacktooth: Breaking through the Defense of Bluetooth in Silence. 2022, https://www.ittc.ku.edu/~bluo/download/ai2022ccs.pdf
18- Bhavith Patnam. Myadam Nishkal Gupta.Design and Implementation of Key Exchange Mechanisms for Software Artifacts using Ocean Protocol . 2022, https://bth.diva-portal.org/smash/get/diva2:1498860/FULLTEXT02.pdf
19- Chiradeep Gupta and N V Subba Reddy, Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography.2022, https://iopscience.iop.org/article/10.1088/1742-6596/2161/1/012014/pdf#:~:text=This%20paper%20proposes%20a%20model,effectiveness%20of%20the%20proposed%20model.
20- Sunny Shrestha,et.al. SoK. A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures. 2022, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3959316_code3631216.pdf?abstractid=3959316&mirid=1
21- ARUP BARUA1et.al. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. 2022,
22- J. Chandrashe et.al. A Comprehensive Study on Digital Signature. 2021, https://www.ijircst.org/DOC/7-a-comprehensive-study-on-digital-signature.pdf
23- Feng Hao, et.al. SoK: Password- Authenticated Key Exchange – Theory, Practice, Standardization and Real-World Lessons . 2021, https://eprint.iacr.org/2021/1492.pdf
24- Bala et.al. A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves Cryptography. 2021, http://dx.doi.org/10.34028/iajit/18/2/6
25- Hannes Salin. Pairing-Based Cryptography in Theory and Practice. 2021, https://www.researchgate.net/publication/366445812_Pairing-Based_Cryptography_in_Theory_and_Practice
26- Svitlana et.al. The Improvement Of Digital Signature Algorithm Based on Elliptic Curve Cryptography. 2021, http://dx.doi.org/10.1007/978-3-030-55506-1_30
27- Shubhani et.al. Digital signatures. 2021, http://dx.doi.org/10.1016/bs.adcom.2020.08.004
28- Mrs. Pratibha Singh, Mr. Dipesh Sharma,Mr. Sonu Agrawal . A Modern Study of Bluetooth Wireless Technology. 2021, https://airccse.org/journal/ijcseit/papers/0811ijcseit06.pdf
29- Michael Troncoso, Britta Hale. The Bluetooth CYBORG: Analysis of the Full Human- Machine Passkey Entry AKE Protocol. 2021, https://eprint.iacr.org/2021/083.pdf
30- Maximilian von Tschirschnitz.Method Confusion Attack on Bluetooth Pairing. 2021, https://doi.org/10.1109/SP40001.2021.00013

31- U.L.Muhammed Rijah et. all. Bluetooth Security Analysis and Solution. 2021, https://www.ijsrp.org/research-paper-0416/ijsrp-p5252.pdf
32-Sai Swaroop Madugula and Ruizhong Wei. An Enhanced Passkey Entry Protocol for Secure Simple Pairing in Bluetooth. 2021, https://doi.org/10.48550/arXiv.2101.09381
33- Ankit B Dubeyet.all. Smart Mobile Attendance System using Bluetooth technology.2021, https://www.irjet.net/archives/V6/i3/IRJET-V6I31344.pdf
34- Asep et.al. Elliptic Curve Diffie-Hellman Cryptosystem for Public Exchange Process. 2020, https://www.ieomsociety.org/detroit2020/papers/523.pdf
35- Asep et.al.Implementation of Elliptic Curve Diffie-Hellman (ECDH) for Encoding Messeges Becomes a Point on the GF(1) . 2020, https://www.researchgate.net/profile/Asep-Saepulrohman/publication/341651515_Implementation_of_Elliptic_Curve_Diffie-Hellman_ECDH_for_Encoding_Messeges_Becomes_a_Point_on_the_GF_1/links/5ecd3302458515294510ffa9/Implementation-of-Elliptic-Curve-Diffie-Hellman-ECDH-for-Encoding-Messeges-Becomes-a-Point-on-the-GF-1.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
36- Eric Järpe. An Alternative Diffie-Hellman Protocol. 2020, https://www.mdpi.com/2410-387X/4/1/5/pdf?version=1585196344
37- Mohammed et.al. Cryptography Survey of DSS and DSA. 2020, http://dx.doi.org/10.1007/978-981-15-1307-7_75
38- Mohan et.al. Key Management Using Elliptic Curve Diffie Hellman Curve 25519, 2020, https://doi.org/10.1109/MPCIT51588.2020.9350454
39- Dwi Liestyowati . Public Key Cryptography. 2020, http://dx.doi.org/10.1088/1742-6596/1477/5/052062
40- Chandra shekhar et.all. Study on Network Security Algorithm.2020, https://www.researchgate.net/profile/Chandrashekhar-Patil-8/publication/354836597_Study_on_Network_Security_Algorithm/links/614eeb6dd2ebba7be747ac12/Study-on-Network-Security-Algorithm.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
41- Vijay, Muthu. A reliable next generation cyber security architecture for industrial internet of things environment. 2020, https://www.researchgate.net/profile/Chellavelu_Vijayakumaran/publication/338971959_A_reliable_next_generation_cyber_security_architecture_for_industrial_internet_of_things_environment/links/5f23c2c1458515b729f5e7d7/A-reliable-next-generation-cyber-security-architecture-for-industrial-internet-of-things-environment.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
42- Gabriel,Everton, Fabiano.An Edge Decentralized Security Architecture for Industrial IoT Applications. 2020, http://dx.doi.org/10.1109/WF-IoT48130.2020.9221176
43- Enis,Eren,Cihat. Design and Implementation of SDN-Based Secure Architecture for IoT-Lab. 2020, http://dx.doi.org/10.1007/978-3-030-36178-5_76
44- Dhieb et. al. Scalable and Secure Architecture for Distributed IoT Systems. 2020, https://arxiv.org/pdf/2005.02456.pdf#:~:text=In%20this%20architecture%2C%20blockchain%20and,stakeholders%20presented%20in%20the%20network.
45- Prescilla, et. al. Sliding Window Block chain Architecture for Internet of Things. 2020, http://dx.doi.org/10.1109/JIOT.2020.2967119
46- Yaniv Shaked and Avishai Wool. Cracking the Bluetooth PIN. 2020, https://www.usenix.org/legacy/event/mobisys05/tech/full_papers/shaked/shaked.pdf
47- Dr. S. V. B. Subrahmanyesw ara Rao, ET.ALL. An Approach to Public- Key Cryptography using Diffie - Hellman Key Exchange Algorithm. 2020
48- David Adrian et.al. Imperfect Forward Secrecy: How Diffie- Hellman Fails in Practice. 2020, https://dl.acm.org/doi/pdf/10.1145/2810103.2813707
49- Tomáš Rosa. Bypassing Passkey Authentication in Bluetooth Low Energy. 2020, https://eprint.iacr.org/2013/309.pdf
50- Yaniv Shaked and Avishai Wool. Cracking the Bluetooth PIN. 2005, https://www.usenix.org/legacy/event/mobisys05/tech/full_papers/shaked/shaked.pdf
51- Richard Chang and Vitaly Shmatikov. Formal Analysis of Authentication in Bluetooth Device Pairing.2020, https://www.cs.cornell.edu/~shmat/shmat_fcs07.pdf

52- Rui Zhang1et.all. The security analysis and improvements of link connection mechanism for mobile phone bluetooth transmission. 2014, https://www.jocpr.com/articles/the-security-analysis-and-improvements-of-link-connection-mechanism-for-mobile-phone-bluetooth-transmission.pdf
53- Heka Bagaskara et.all. Proximity and Dynamic Device Pairing based Authentication for IoT Devices with Decision Tree Method.2020, **DOI:** 10.1109/ICIDM51048.2020.9339643
54- Dr.M.AMANULL AH1, R.LAVANYA2. Bluetooth Enabled Robot Using Smart Phone During Disaster. 2018, https://www.jetir.org/papers/JETIR1804435.pdf
55- Gerhard Klostermeier and Matthias Deeg. Security of Modern Bkuetooth Keyboards. 2018, https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Security_of_Modern_Bluetooth_Keyboards.pdf
56- J. T. Lalis, et.al. Securing Bluetooth. 2014, https://www.researchgate.net/profile/Bobby-Gerardo-2/publication/282829872_Securing_Bluetooth_Communication_with_Hybrid_Pairing_Protocol/links/58f488e8458515ff23b497db/Securing-Bluetooth-Communication-with-Hybrid-Pairing-Protocol.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
57- Bijoy Kumar et.al . Architecture Design for Wireless Authentication Security in Bluetooth Network. 2014, https://www.researchgate.net/profile/Bijoy-Mandal/publication/282829975_An_Architecture_Design_for_Wireless_Authentication_Security_in_Bluetooth_Network/links/56d57e9c08ae78702deb4ed8/An-Architecture-Design-for-Wireless-Authentication-Security-in-Bluetooth-Network.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
58- Mrs. ranbir kaur. Applications Transforming Technology of future Bluetooth. 2014
59- Konstantinos et. al. Architectural Patterns for Secure IoT Orchestrations. 2019, https://www.researchgate.net/profile/Konstantinos-Fysarakis-2/publication/334416246_Architectural_Patterns_for_Secure_IoT_Orchestrations/links/5d2c161a92851cf44084ff97/Architectural-Patterns-for-Secure-IoT-Orchestrations.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
60- Krishna et all. SDN Enabled Secure IoT Architecture.2019, https://dl.ifip.org/db/conf/im/im2019short/188667.pdf
61- Dr.Ahmad Hweishel A.Alfarjat et. al. Implementation of Bluetooth Secure Simple Pairing (SSP) using Elliptic Curve Cryptography (ECC). 2021, http://paper.ijcsns.org/07_book/202103/20210309.pdf
62- Praveen Kumar Mishra. Analysis Of MITM Attack In Secure Simple Pairing. 2013, https://www.rroij.com/open-access/analysis-of-mitm-attack-in-secure-simple-pairing-42-45.pdf
63- Mohit Sethi_y, et.al. Device pairing with synchronized drawing. 2014, https://www.researchgate.net/figure/Synchronized-drawing-for-device-pairing_fig1_269307474/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6Il9kaXJlY3QifX0
64- Jethro Beekman, et.al. A technical report on "man-in-the- middle attack" on t-mobile wi-fi calling.2013, https://www2.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-18.pdf
65- Eddie LaCost. Automating Bluetooth Pairing via Near-Field Communications (NFC). 2016, https://www.ti.com/lit/an/sloa187a/sloa187a.pdf?ts=1706805312602&ref_url=https%253A%252F%252Fwww.google.co.in%252F
66- Shivappa et.al. General approach for bluetooth network security system. 2013. https://www.academia.edu/4138395/GENERAL_APPROACH_FOR_BLUETOOTH_NETWORK_SECURITY_SYSTEM 67- Durresi et. al. Secure communication architecture for internet of things using smartphones and multi-access edge computing in environment monitoring. 2013
68- Tibursk et. al. Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices. 2013, **DOI:** 10.1109/MCOM.2018.1701047
69- Tzu-Chang Yeh, et.al. Securing Bluetooth Communications. 2012, http://ijns.jalaxy.com.tw/contents/ijns-v14-n4/ijns-2012-v14-n4-p229-235.pdf
70- Nishant Mishra et.al. Overview Of Bluetooth Security. 2012, https://www.ijcset.com/docs/IJCSET12-03-06-043.pdf
71- Delan Alsoufi, et.al. Improving the leap protocol. 2012, https://www.researchgate.net/profile/Khaled-Elleithy/publication/256455725_Security_In_Wireless_Sensor_Networks_-

_Improving_The_LEAP_Protocol/links/02e7e522bbb1f7a161000000/Security-In-Wireless-Sensor-Networks-Improving-The-LEAP-Protocol.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
72- K. VamsiRam et.al. Network Security Management in Wireless Networks through Zero Knowledge Proof. 2015, https://www.academia.edu/41448304/Analysis_of_Ad_Hoc_Network_Security_using_Zero_knowledge_Proof_and_Wi_Fi_Protected_Access_2
73- Lucas Jacob, et.al. Wi- fi security: wireless with confidence. 2011, https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1018&context=asi
74- Mr.K.Saravanan, et.al. A Novel Bluetooth Man-In-The- Middle Attack Based On SSP using OOB Association model. 2012, https://arxiv.org/ftp/arxiv/papers/1203/1203.4649.pdf
75- Mahendra Kumar et.al. A Study of Wireless Ad-Hoc Network attack and Routing Protocol attack. 2012,https://www.academia.edu/es/1642786/A_Study_of_wireless_Ad_Hoc_Network_attack_and_Routing_Protocol_attack
76- A.Antony et.al. Checking security of WPE and WPA. 2012
77- Sanjay Kumar et.al. Security on Voice over Internet Protocol from Spoofing attacks. 2012, https://ijarcce.com/wp-content/uploads/2012/06/A-Review-Paper-Security-on-Voice-over-Internet-Protocol-from-Spoofing-attacks.pdf
78- C. Krishna et.al. Safety measures against man-in- the-middle attack In key exchange. 2012, https://www.researchgate.net/profile/G-Jose-2/publication/289763478_Safety_measures_against_man-in-the-middle_attack_in_key_exchange/links/59ca0237aca272bb050747e5/Safety-measures-against-man-in-the-middle-attack-in-key-exchange.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
79- Pushpendra Kumar et.al. Analysis on Man in the Middle Attack on SSL. 2012, https://www.researchgate.net/profile/Srijith-S-Kumar/publication/228333979_Analysis_on_Man_in_the_Middle_Attack_on_SSL/links/0912f4ffa600447d29000000/Analysis-on-Man-in-the-Middle-Attack-on-SSL.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
80- Mahendra Kumar et.al. A Study of wireless Ad-Hoc Network attack and Routing Protocol attack. 2012,https://www.academia.edu/es/1642786/A_Study_of_wireless_Ad_Hoc_Network_attack_and_Routing_Protocol_attack
81- G. RAMESH, et.al. A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation.2012, https://www.researchgate.net/publication/292567250_UR5_A_novel_symmetrical_encryption_algorithm_with_fast_flexible_and_high_security_based_on_key_updation
82- Nateq Be-Nazir et.al. Bluetooth security threats and solutions: a survey. 2012,https://www.researchgate.net/profile/Mohammed-Tarique-2/publication/267200901_Bluetooth_Security_Threats_And_Solutions_A_Survey/links/555d822b08ae6f4dcc8c39b3/Bluetooth-Security-Threats-And-Solutions-A-Survey.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
83- Nishant Mishra et.al. Defense against MAN IN MIDDLE ATTACK In Secure Simple Pairing. 2012, https://www.researchgate.net/publication/278003247_DEFENCE_AGAINST_MAN_IN_MIDDLE_ATTACK_IN_SECURE_SIMPLE_PAIRING
84- Vinayak P. Musale, et.al. Security risks in Bluetooth devices. 2012, https://research.ijcaonline.org/volume51/number1/pxc3881308.pdf
85- Thrinatha R et.al. Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing. 2011
86- K. Haataja, et.al. Man-in-the-Middle Attacks against Bluetooth Secure Simple Pairing. 2008, https://doi.org/10.1109/WiCom.2008.1153
87- Imam AL Momani, et.al. Secure public key exchange against man- in-the- middle attacks during simple secure pairing (SSP). 2011, https://www.researchgate.net/profile/Mousa-Al-Akhras/publication/261706337_Secure_Public_Key_Exchange_against_Man-In-The-Middle_Attacks_during_Secure_Simple_Pairing_SSP_in_Bluetooth/links/02e7e535168a7351d9000000/Secure-

Public-Key-Exchange-against-Man-In-The-Middle-Attacks-during-Secure-Simple-Pairing-SSP-in-Bluetooth.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
88- M Thrinatha Reddy, et.al. Man- in-the- Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing. 2011, https://core.ac.uk/reader/53188050
89- Carsten Maple, et.al. Number of weaknesses in existing protocols and configurations. 2007 , https://www.researchgate.net/profile/Yong-Yue/publication/220166022_Reliability_Availability_and_Security_of_Wireless_Networks_in_the_Community/links/00b7d53b932ed143b2000000/Reliability-Availability-and-Security-of-Wireless-Networks-in-the-Community.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
90- Anthony C. Ijeh, et.al. Security Measures in Wired and Wireless Networks. 2009, https://www.researchgate.net/profile/Anthony-Ijeh/publication/260789564_Security_Measures_in_Wired_and_Wireless_Networks/links/604f835f458515e8344a4443/Security-Measures-in-Wired-and-Wireless-Networks.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
91- Raj Kumar Singh, et.al. A survey of security mechanisms. 2010
92- Tarun Kumar. Problem of pin guessing attack on the Bluetooth system. 2009, https://www.researchgate.net/profile/Tarun-Kumar-17/publication/228342859_Improving_Pairing_Mechanism_in_Bluetooth_Security/links/593b7b19a6fdcc17a9b73189/Improving-Pairing-Mechanism-in-Bluetooth-Security.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
93- Prof. (Dr.) Khanna et.al. Wireless home security system with mobile. 2009, https://www.technicaljournalsonline.com/ijeat/VOL%20II/IJAET%20VOL%20II%20ISSUE%20IV%20%20OCTBER%20DECEMBER%202011/ARTICLE%2066%20IJAET%20VOLII%20ISSUE%20IV%20OCT%20DEC%202011.pdf
94- Yasir Arfat et.al. A tool for analysis of device pairing methods. 2009, https://www.semanticscholar.org/reader/b56ec0204b24c474493a3cb675dcb9e4bdf7a0ce
95- Claudio Soriente, et.al. Secure pairing of interface constrained devices. 2009, https://www.researchgate.net/profile/Ersin-Uzun-2/publication/220080819_Secure_pairing_of_interface_constrained_devices/links/0912f5142c2d364381000000/Secure-pairing-of-interface-constrained-devices.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
96- Arun Kumar, et.al. A comparative study of secure device pairing methods. 2009, https://doi.org/10.1016/j.pmcj.2009.07.008
97- Min-kyu Choi1, et.al. Network Security, Vulnerabilities, Threats and Countermeasures. 2008, https://www.researchgate.net/profile/Rosslin-Robles/publication/228864040_Wireless_Network_Security_Vulnerabilities_Threats_and_Countermeasures/links/5ceb95bc92851c4eabc1219f/Wireless-Network-Security-Vulnerabilities-Threats-and-Countermeasures.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
98- Claudio Soriente, et.al. Human-Assisted Pure Audio Device Pairing. 2007, https://eprint.iacr.org/2007/093.pdf
99- Ersin Uzun et.al. Usability Analysis of Secure Pairing Methods. 2007, https://www.researchgate.net/profile/Ersin-Uzun-2/publication/220796820_Usability_Analysis_of_Secure_Pairing_Methods/links/0912f5142c2d2e30f0000000/Usability-Analysis-of-Secure-Pairing-Methods.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
100- Selim Aissi, et.al . Enhancing Bluetooth Security Using an Improved Pairing Mechanism.2004, ftp://195.238.226.35/tsg_sa/WG3_Security/TSGS3_34_Acapulco/Docs/PDF/S3-040481.pdf.