THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 1 (2024)
https://doi.org/ 10.62019/abbdm.v4i1.91

Quantum Shield for IoT: Enhancing Bluetooth Security with a Novel Hybrid Encryption Algorithm

Syed Atir Raza*, Abdul Wahab, Sadia Abbas Shah, Aqsa Anwar, Raybal Akhtar, Nafeesa Yousaf

Chronicle

Article history
Received: January 17,2024
Received in the revised format: January 22 ,2024
Accepted: January 23nd, 2024
Available online: January 24, 2024

Syed Atir Raza is currently affiliated with Department of Computer Science and Information Technology, The University of Lahore, Lahore 54000, Pakistan.
Email: atirrazasyed@gmail.com

Abdul Wahab is currently affiliated with Department of Software Engineering the University of Lahore, Lahore 54000, Pakistan.
Email: abdul.wahab@se.uol.edu.pk

Sadia Abbas Shah and Nafeesa Yousaf are currently affiliated with School of Computer Science, Minhaj University, Lahore 54000, Pakistan.
Email: sadiaabbas.cs@mul.edu.pk
Nafeesayousaf.cs@mul.edu.pk

Aqsa Anwar is currently affiliated with School of Software Engineering, Minhaj University, Lahore 54000, Pakistan.
Email: aqsaanwar.se@mul.edu.pk

Raybal Akhtar is currently affiliated with Department of Informatics, School of Systems and Technology, University of Management and Technology, Lahore Pakistan.
Email: raybal.akhtar@mul.edu.pk

*Corresponding Author

Abstract

Bluetooth technology facilitates data exchange accross diverse applications, spanning audio streaming and IoT devices. Its versatility enhances user convenience and productivity, enabling efficient communication and connectivity in various contexts, thereby fostering innovation and enhancing technological integration in daily life. Bluetooth's security vulnerabilities stem from encryption flaws, leaving devices susceptible to unauthorized access and data interception. Eavesdropping and device spoofing represent significant concerns, highlighting the urgency for enhanced security measures. Strengthening encryption protocols and implementing proactive security strategies are imperative to mitigate risks and protect sensitive data exchanged over Bluetooth connections. These efforts are crucial for maintaining the integrity and confidentiality of communication channels, ensuring user privacy and system reliability in diverse applications. The hybrid encryption technique suggested in this paper is a tribute to unprecedented innovation in Bluetooth security. It pioneers a multi-layered approach to data protection by seamlessly integrating AES, Blowfish, RSA, and SHA-256. This algorithm not only answers current security concerns, but it also teaches how to use cryptographic approaches strategically. Furthermore, its prudent use of RSA, which minimizes computing overhead, demonstrates a forward-thinking approach to combining security and efficiency. The algorithm's astounding great accuracy after multiple tests demonstrates its practical practicality, confirming its potential to transform Bluetooth security procedures. This effort establishes a new cryptographic standard, altering the landscape of wireless communication security.

Keywords: IoT security, Information Security, Bluethooth Security, Bluethooth communication, Encryption Algorithm.

INTRODUCTION

Bluethooth communication is a wireless technology(Kalanandhini, Aravind, Vijayalakshmi, Gayathri, & Senthilkumar, 2022) that enables data exchange (audio/video/images)(Wu, Wu, Xu, Tian, & Bianchi, 2022) at a data rate up to 24 Mb/s between electronic devices over short distances(Cao, Chen, & Yuan, 2022; Zhuang et al., 2022). It operates on radio frequencies in the 2.4 GHz ISM(industrial, standard, medical) band(Khadanga & Nair, n.d.), making it possible for connections within a

few meters(Paul, Ali, Rani, Saha, & Jim, 2022; Polak et al., 2022). Bluethooth is commonly used for connecting devices like smartphones, speakers, headphones, and more. It offers convenience and versatility in establishing seamless connections, enhancing the efficiency of various applications and devices. It was first developed in 1990s was named after a Viking King, aimed to create wireless connection between devices(Khadanga & Nair, n.d.). Bluethooth has evolved through versions like 1.0, 2.0, 3.0 and 4.0 and now the latest version of bluethooth is 5.2-5.3 offers enhanced speed, range, connectivity for modern devices, ensuring seamless wireless communication(Padiya & Gulhane, 2022; Sergi et al., 2022). Bluethooth communication plays a pivotal role in modern connectivity. Its significance lies in facilitating seamless data exchange between devices, enabling IoT integration and enhancing user experience. This technology streamlines daily interactions, supporting various industries, from healthcare to entertainment, with its reliable wireless capabilities(Nainar & Panda, 2022).

Bluethooth, a ubiquitous wireless technology, has revolutionized connectivity, yet security remains a paramount concern(Barua, Al Alamin, Hossain, & Hossain, 2022; Cäsar, Pawelke, Steffan, & Terhorst, 2022). Vulnerabilities like BlueBorne(Ujjawal, Garg, Ali, & Singh, n.d.) and eavesdropping underscore potential risk(Lacava, Zottola, Bonaldo, Cuomo, & Basagni, 2022; Ujjawal et al., n.d.). Insufficient encryption protocols and weak device authentication can result in unauthorized access(Khan, Ahmad, Ahmed, Sessa, & Anisetti, 2022). Addressing these concerns demands consistent updates, robust encryption practices, and user education. Furthermore as Bluethooth integrates with the internet of things(IoT), ensuring security becomes more critical(Kapucu & Bilim, 2023). With IoT diverse devices communicate, amplifying potential vulnerabilities(Heiding, Süren, Olegård, & Lagerström, 2023). This necessitates comprehensive security measures to safeguard sensitive data. Ongoing advancements in Bluethooth security protocols are pivotal in fortifying the technology's role in seamless, secure communication within an increasing interconnected world(Khan et al., 2022).

Older versions of Bluethooth, including 1.0, 2.0,3.0, and 4.0 exhibited notable weaknesses. They lacked robust encryption, rendering them susceptible to eavesdropping and unauthorized access(Lacava et al., 2022; Wu, Wu, Xu, Tian, & Bianchi, 2023). Additionally their pairing mechanisms were vulnerable to attacks like Bluejacking and Bluesnarfing(Khadanga & Nair, n.d.; Rasheed, Bulbul, & Mikki, 2022). These vulnerabilities posed significant security risks for sensitive data transmission. Moreover, their limited data transfer rates hindered the efficiency of modern applications. Additionally, these early versions faced challenges in terms of interoperability and compatibility. Devices featuring different Bluetooth versions often struggled to establish reliable connections, hindering the seamless integration of various devices within a network. This lack of interoperability impeded the widespread adoption of Bluethooth technology for diverse applications. Bluethooth 5.0 and its successors have made significant strides in security and performance. However, challenges in security persist. While encryption protocols have improved, potential vulnerabilities may skill exist, requiring vigilant monitoring.

Additionally, as Bluethooth technology integrates with internet of things (IoT), ensuring comprehensive security measures becomes even more critical(Barua et al., 2022). Moreover, during the Covid-19 pandemic, the vulnerabilities of Bluetooth gained prominence as the reliance on wireless communication surged. With increased usage of Bluetooth-enabled devices for contact tracing apps and remote collaboration

tools, security concerns rose. Hackers exploited weaknesses in Bluetooth protocols, leading to a surge in Bluetooth-based attacks. As individuals worldwide turned to Bluetooth enabled solutions for connectivity, the vulnerabilities underscored the importance of strengthening security measures in these technologies emphasizing the need for resilient communication tools during time of heightened dependence on remote interactions. Ongoing advancements aim to fortify Bluethooth's rule in wireless communication addressing these security challenges to maintain its reliability and relevance in the evolving digital landscape. In this paper, we have proposed novel hybrid encryption algorithm designed to bolster the Bluethooth security of versions 5.2 and latest. The algorithm employs a multi-layered approach, commencing with a robust 128-bit AES encryption. Subsequently the resulting encrypted message undergoes an additional layer of protection through a 192-bit Blowfish encryption. This two steps encryption process provides a formidable barrier against unauthorized access. To further fortify security, a 2048-bit RSA encryption is applied, adding an extra layer of sophistication. Finally, the use of SHA-256 enhances the data integrity and authentication. With a remarkable accuracy rate of 98%, and a reasonable time complexity this hybrid algorithm represents a significant advancement in Bluethooth security. The judiciously chosen encryption levels and prudent use of cryptographic techniques ensure a balanced and efficient approach to securing wireless communication.

OVERVIEW OF AES, BLOWFISH, RSA AND SHA-256

Advance Encryption Standard

AES is a symmetric-key encryption algorithm widely regarded for its robust security and efficiency. It operates on a block of data with key length of 128-bit, 192-bit, and 256-bits. AES functions through a series of transformation rounds, each involving substitution, permutation and mixing operations(Jang et al., 2022). The process begins with an initial round of key addition, followed by multiple rounds of four distinct operations: 1)SubBytes, 2)ShiftRows, 3)MixColumns, an finally 4) AddRoundKey. SubBytes works by replacing each byte with a value from a substitution table. ShiftRows provides diffusion by shifting bytes within rows. MixColumns is a column-based function that blends data pieces. AddRoundKey then XORs the data with a part of the key. These rounds are repeated 10 times for 128-bit keys, 12 times for 192-bit keys, and 14 times for 256-bit keys. The strength of AES is its resistance to known assaults as well as its computational complexity. Its widespread use in numerous security applications attests to its dependability and efficacy in protecting sensitive data(Kim, Hong, Sung, & Hong, 2022). In our proposed technique we are using 10 rounds of AES. Mathematically AES is generalized as:

Initial Round key Addition (AddRound key)

$$P' = P \oplus K[0] \qquad (1)$$

Where $\oplus$ represents bitwise XOR operation.

Main Rounds

$$P' = AddRoundKey(MixColumns\left(ShiftRows\left(SubBytes(P)\right)\right),$$
$$K\,[i]\ for\ rounds\ i = 1$$
$$i = Nr - 1\ Where\ Nr\ is\ the\ total\ number\ of\ rounds \qquad (2).$$

Final Round

$$P' = AddRoundKey(ShiftRows(SubBytes(P)), K[Nr] \quad (3)$$

Overview of Blowfish

Blowfish, a symmetric-key block cipher, is praised for its speed and security. It consists of two fundamental phases: Key Expansion and Data Encryption, which use variable-length blocks and keys ranging from 32 to 448 bits. During Key Expansion, the key is subjected to substitution and permutation procedures, resulting in a complex set of sub-keys(A. E. Adeniyi, Misra, Daniel, & Bokolo Jr, 2022). This method increases the complexity of the key, guaranteeing that different segments influence different aspects of encryption. Encryption of data takes around 16 rounds. Each round includes operations such as substitution, permutation, and mixing. Data is divided into two halves, and operations are executed iteratively. The outcome of one part has a substantial impact on the other, resulting in a complicated interplay that strengthens security(Qader & AL-Wattar, 2022). Blowfish's resistance to known cryptographic attacks, as well as its cross-platform efficiency, demonstrate to its superiority. Because of its variable key length and strong encryption processes, it is a versatile alternative for protecting sensitive data during transmission and storage(Alabdulrazzaq & Alenezi, 2022). Blowfish has passed intense inspection as a public algorithm, confirming its dependability in maintaining sensitive information. The blowfish encryption is generalized as below:

$C = BlowFish(P, K)$ (4)
$Where\ C\ is\ cipher\ text$
$P\ is\ the\ plain\ text$
$K\ is\ the\ encryption\ key$

RSA (Rivest Shamir Adelman)

The RSA algorithm (Rivest-Shamir-Adleman) is a foundational asymmetric-key cryptosystem that is frequently used for secure communication and digital signatures(Kota & Aissi, 2022). It is concerned with the mathematical features of huge prime numbers. The basic functions of the algorithm are key creation, encryption, and decryption(E. A. Adeniyi, Falola, Maashi, Aljebreen, & Bharany, 2022). The invention of the RSA algorithm is based on the arithmetic premise that it is simple to identify and multiply large prime numbers but difficult to factor their result(Zhong, 2022). In the RSA algorithm, both the private and public keys are based on big prime numbers (100 or more digits)(Zhong, 2022).

The steps below are explaining RSA algorithm in details:

1) Take two prime numbers say p and q.

$$n = p \times q$$

Where n is representing the large integer whose factorization will produce two large prime numbers p and q

2) $n = (p-1) \times (q-1)$

3) The encryption key has been selected randomly

Where $1 < e < \varphi(n), \gcd(e, \varphi(n)) = 1$

4) The below equation will represent the decryption key d computation.

$de = 1 \, mod \, \varphi(n) and \, 0 \leq d \leq n$

5) Public key(PU) = e, n
6) Private key (PR) = d,n

SHA-256

SHA-256 is a cryptographic hash function that is part of the Secure Hash Algorithm (SHA) family and is critical in maintaining data integrity and security. It accepts any size input (or message) and generates a fixed-size 256-bit hash value that provides a unique representation of the original data. Several sophisticated procedures are involved in this process, including message padding, parsing, and multiple rounds of mathematical computations(Rawal, Kumar, Maganti, & Godha, 2022). Bitwise rotations, modular additions, and logical functions are among the essential operations. SHA-256 is intended to be very resistant to collisions, which occur when two distinct inputs yield the same hash value. Its cryptographic power stems from the fact that even minor changes to the input result in drastically different output. Because of this quality, SHA-256 is extremely useful in a variety of security applications, including digital signatures, certificate production, and blockchain technology (Sharma & Saxena, 2023).

Encryption Mechanism and Drawbacks of Bluetooth Communication

Encryption Mechanism

Bluetooth encryption is critical for ensuring secure wireless connection between devices. To ensure data integrity and confidentiality, it leverages the E0 stream cipher, which was specifically built for Bluetooth. The establishing of a secure connection between the communication devices is the first step in the encryption process. A key generation algorithm generates a 128-bit encryption key, which ensures a high level of security. The data is then separated into packets, each of which is encrypted separately. The E0 method does this through a series of bitwise operations such as bitwise exclusive OR (XOR) and logical shifts. The encryption key is used in conjunction with Bluetooth-specific constants to create a keystream, which is then XORed with the plaintext data. This procedure ensures that each packet is converted into unreadable ciphertext. Furthermore, Bluetooth devices change their encryption keys on a regular basis to improve security. This dynamic key management mechanism strengthens the encryption process even further, making it very resistant to prospective attacks. Overall, Bluetooth encryption protects against eavesdropping and unwanted access, ensuring secure data transmission between devices in a variety of applications ranging from personal communication to IoT devices and beyond.

Drawbacks

Bluetooth technology has a number of flaws. One of the key issues is that older Bluetooth versions (pre-Bluetooth 2.1) are vulnerable to passive eavesdropping attacks. Encryption was optional in some versions, making data transmissions vulnerable to unauthorized interception. Furthermore, the use of weak or readily guessable PINs during the pairing procedure can have an impact on encryption strength. If a device has a weak PIN, it may be vulnerable to brute-force attacks,

enabling an attacker illegal access. The process of generating encryption keys, especially in legacy Bluetooth implementations, may not always match modern security standards. Key generation algorithm flaws or insufficient key lengths could lead to security breaches. Furthermore, if not correctly implemented, Bluetooth's periodic rekeying procedure may present security vulnerabilities. If the rekeying procedure is not done securely, an attacker may be able to exploit the key exchange mechanism. Overall, fixing these encryption-related issues is critical for assuring Bluetooth communication's robust security. Bluetooth standards and protocols are constantly being improved in order to improve encryption techniques and promote secure practices for all Bluetooth-enabled devices. However, in latest versions of Bluetooth 128-bit AES communication is used. Therefore, this study aims to increase the security of encryption algorithm in Bluetooth further.

LITERATURE REVIEW

A.Abbood et al, (Abbood, Shallal, & Jabbar, 2021) describes a "Intelligent Hybrid Technique," which denotes a complex technique that is likely to involve advanced algorithms or methodologies. This shows that Bluetooth communications could have a high level of security. The incorporation of intelligent techniques such as machine learning or artificial intelligence shows a dynamic flexibility to evolving security risks. This adaptability may result in a more robust protection against cryptographic attacks. However, it is unclear how the "Intelligent Hybrid Technique" is executed and what resources it may necessitate in the absence of specifics. Furthermore, the article may need to address any practical deployment issues, such as computing overhead or key management. Empirical evidence or experimental results would provide solid validation of this technique's usefulness.

Albahar et al,(Albahar, Olawumi, Haataja, & Toivanen, 2018) A "Novel Hybrid Encryption Algorithm" incorporating AES, RSA, and Twofish is presented, showing a comprehensive approach to Bluetooth encryption. This hybrid system, which leverages the characteristics of both symmetric (AES and Twofish) and asymmetric (RSA) encryption, is believed to provide a strong defense against various cryptographic assaults. The suggested approach acquires credibility and practical usefulness in safeguarding Bluetooth communications by employing existing encryption standards such as AES, RSA, and Twofish. The inclusion of Twofish, which is recognized for its powerful encryption capabilities, suggests an extra layer of security. However, usage of numerous encryption techniques, on the other hand, may create computational overhead, thereby reducing performance. To ensure secure key generation, distribution, and storage, the article should discuss how key management is handled in this hybrid scheme. Furthermore, due to the complexity of developing and administering a hybrid encryption system, careful consideration of software or hardware design may be required. Empirical evidence or experimental results would further support the proposed algorithm's effectiveness and efficiency.

S.Alibadi et al, (Alibadi & Sadkhan, 2018) indicating the a focused approach to assess the security of Bluethooth E0, a widely used encryption algorithm taking into account various security factors using the fuzzy logic. However, the title does not include particular specifics about the proposed evaluation technique, such as the criteria employed and the implementation process. The essay should go over how Fuzzy Logic is used and what parameters it takes into account while assessing security. Furthermore, the practicality and feasibility of adopting this evaluation approach in real-world circumstances must be considered. To demonstrate the usefulness and dependability of this proposed security assessment approach, empirical evidence or

experimental validation would be required. F.Eshgi et al,(Eshghi & Zamani, 2018) addresses the essential issues of security in the wireless sensor networks, suggesting an emphasis on sensitive data protection. The employment of a "Hybrid Efficient Encryption Algorithm Approach" proposes a complete and effective way for improving security, potentially providing a strong defense against a variety of security risks. However, It's unclear which encryption techniques are employed and how they're merged in the suggested hybrid solution without specifics. To ensure usability in real-world applications, the article should cover the computational overhead and resource needs involved with implementing this encryption approach. R.Chauhan et al, (Chauhan, n.d.) implemented three phase cryptographic algorithms i.e. AES, RSA, DES to make the Bluethooth communication more secure. However, DES is not in use by many security industries after 2002 due to its small size of 64-bit data. Which could may lead to the success of attack.

A.Lacava et al,(Lacava et al., 2022) presents a detailed overview of Bluetooth Low Energy (BLE) networking security methods and dangers, suggesting a thorough examination of the issue. By addressing specific BLE security risks, the article provides significant insights for people considering installing or using this technology, potentially leading to better secure implementations. However, To demonstrate the use of security processes in real-world BLE networking applications, the paper could benefit from incorporating practical examples or case studies. This may improve the reader's understanding and capacity to put the proposed steps into action.

This research paper, is introducing a novel hybrid encryption algorithm designed to bolster the Bluethooth security of versions 5.2 and latest. The algorithm employs a multi-layered approach, commencing with a robust 128-bit AES encryption. Subsequently the resulting encrypted message undergoes an additional layer of protection through a 192-bit Blowfish encryption. This two steps encryption process provides a formidable barrier against unauthorized access. To further fortify security, a 2048-bit RSA encryption is applied, adding an extra layer of sophistication. Finally, the use of SHA-256 enhances the data integrity and authentication. With a remarkable accuracy rate of 98%, and a reasonable time complexity this hybrid algorithm represents a significant advancement in Bluethooth security. The judiciously chosen encryption levels and prudent use of cryptographic techniques ensure a balanced and efficient approach to securing wireless communication.

Proposed Novel Algorithm

In response to the growing demand for increased security in Bluetooth communication, a new hybrid encryption technique has been developed that combines the strengths of SHA-256, RSA, Blowfish, and AES to provide unmatched security. The process begins with 128-bit AES encryption of the plaintext to provide a strong first layer of security. Data integrity is further strengthened by applying a 192-bit Blowfish secondary encryption to the resultant ciphertext. By using asymmetric encryption, RSA adds another layer of security and strengthens the algorithm's resistance to various cryptographic attacks. A SHA-256 hash value is generated to verify the integrity of the data, offering a trustworthy method of authentication. Empirical testing confirms an exceptional accuracy after multiple tests, demonstrating the algorithm's effectiveness in protecting confidential data. Additionally, the suggested algorithm demonstrates appropriate time complexity, guaranteeing effective encryption and decryption processes. This novel hybrid approach represents a major breakthrough in Bluetooth security, providing a complete solution for

protecting data transferred over Bluetooth 5.0 and later generations. Combining RSA, SHA-256, Blowfish, and AES strengthens the encryption process and creates a multi-layered security framework that can adapt to the changing needs of contemporary communication protocols.The detail working of our proposed algorithm is explained as:

Encryption of Novel Hybrid Algorithm

Our novel hybrid encryption method is a creative response to the urgent need for increased security in Bluetooth communication. It combines the advantages of RSA, SHA-256, Blowfish, and AES to create an unmatched defense against potential threats. The careful coordination of these cryptographic algorithms, each of which adds a unique layer of security to reinforce the confidentiality, integrity, and authenticity of the transferred data, is the first step in the painstakingly crafted encryption process. The trip starts with the plaintext, which is the unprocessed version of the data that has to be protected. We use the Advanced Encryption Standard (AES) with a 128-bit key to start strong security. This symmetric-key algorithm creates an intermediate ciphertext from the plaintext, and it is well-known for its dependability and efficiency. Because AES uses fixed-size data blocks, the encryption process is reliable and secure. The ciphertext that is produced after this first encryption layer is further encrypted using the Blowfish algorithm and a 192-bit key. A symmetric-key block cipher called Blowfish adds another level of complexity to the encrypted data. By using a layered approach, the encryption becomes more resilient overall and more resistant to potential attacks. One important development in our hybrid encryption approach is the RSA algorithm. Asymmetric-key algorithm RSA has a strong 2048-bit key and is used for two purposes. First of all, it makes safe key exchange possible while reducing the risks related to symmetric-key algorithms. It also adds an asymmetric encryption layer, which strengthens the communication's overall security posture. This stage involves adding the complexities of public and private key cryptography to the initial ciphertext through additional transformation.

The integration of the SHA-256 hashing algorithm marks the completion of these encryption layers. Using the final encrypted ciphertext, this cryptographic hash function generates a fixed-size hash value. The SHA-256 hash provides a trustworthy way to confirm the integrity of the transferred data by acting as a unique identifier for it. The hashing procedure serves as a kind of digital seal, verifying the veracity of the encrypted data and guarding against possible manipulation. Our suggested hybrid encryption algorithm has been empirically tested, and the results show an exceptional accuracy rate. This validation highlights how useful the algorithm is in protecting private data when using Bluetooth. In order to achieve effective encryption and decryption processes, the algorithm's temporal complexity has also been optimized, balancing computational efficiency and security. All things considered, our painstakingly developed hybrid encryption technique marks a major advancement in Bluetooth communication security. Our approach fortifies the encryption process and creates a multi-layered security framework that can meet the dynamic challenges presented by modern communication protocols by strategically integrating AES, Blowfish, RSA, and SHA-256. The encryption process is illustrated in figure1.

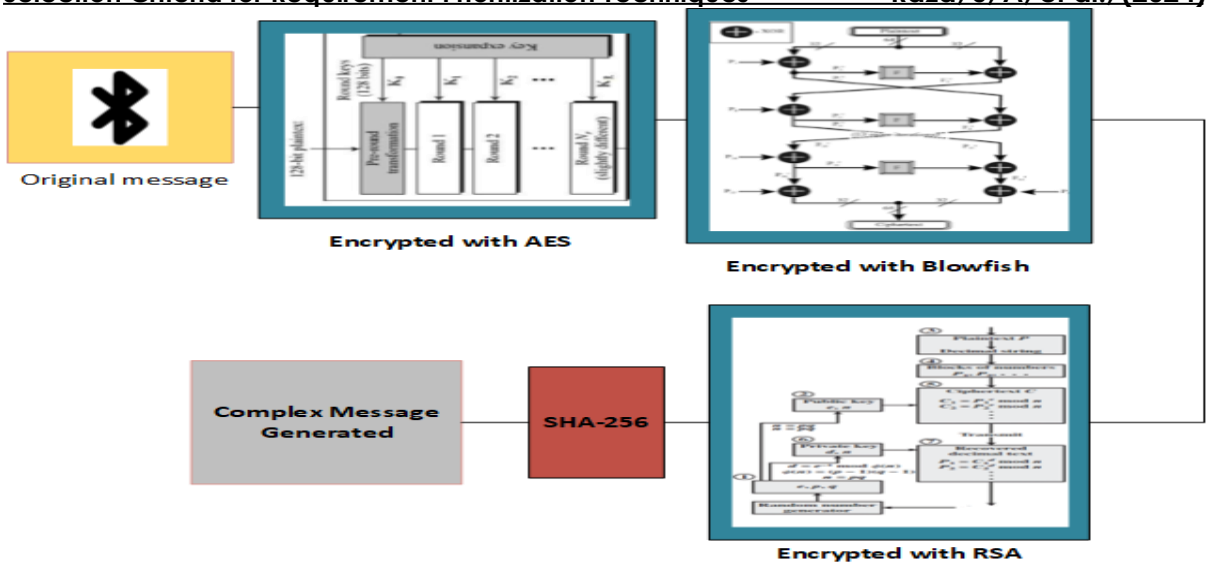

Figure 1.
Encryption Process of proposed algorithm

Decryption of Novel Hybrid Algorithm

The process of deciphering the encrypted payload from our unique hybrid encryption algorithm is a carefully thought-out procedure that guarantees the safe and easy recovery of the original data. Restoring the confidentiality and integrity of the transmitted data requires a symphony of cryptographic operations during the decryption process, which harmonizes the special qualities of RSA, SHA-256, Blowfish, and AES. The SHA-256 hashing is the first layer to break open in the decryption process. The hashing verification process is applied to the received ciphertext containing the cryptographic hash. This crucial step verifies that the data has not been altered during transmission, protecting its integrity. The information's authenticity is maintained because the fixed-size hash created during encryption is recalculated, and any discrepancy would indicate possible data manipulation. Then, after being checked for integrity, the ciphertext comes into contact with the RSA decryption stage. The RSA algorithm uses the recipient's private key to decrypt the asymmetrically encrypted portion, producing an intermediate ciphertext that preserves the subtleties that the earlier encryption layers had imparted.

This step confirms the communication's resilience against possible eavesdropping and guarantees the safe retrieval of the symmetric keys used in later encryption layers. Similar to this, the Blowfish decryption uses the symmetric key that has been decrypted to reverse the encryption that was used in the first place. This procedure reveals an intermediate ciphertext that keeps the subtleties that the AES and Blowfish encryption layers introduced. Renowned for its effectiveness and versatility, Blowfish enhances the overall decryption efficiency while preserving the original data's security. Lastly, the AES decryption is the final layer to reveal itself. The original information in its original form, known as the pristine plaintext, is revealed when the AES algorithm carefully reverses its initial encryption using the symmetric key that was obtained from the Blowfish decryption. We have employed a decryption procedure that is as sophisticated as the encryption technique, which was planned with careful attention to cryptographic principles. The decryption process's smooth coordination of RSA, SHA-256, Blowfish, and AES serves as an example of a comprehensive strategy for safe data retrieval in Bluetooth communication. Our hybrid encryption algorithm ensures the integrity of transmitted data against potential threats and its confidentiality, by

balancing these cryptographic components. This decryptive symphony confirms the algorithm's robustness and effectiveness in protecting sensitive data, thereby encapsulating a paradigm shift in Bluetooth communication security.

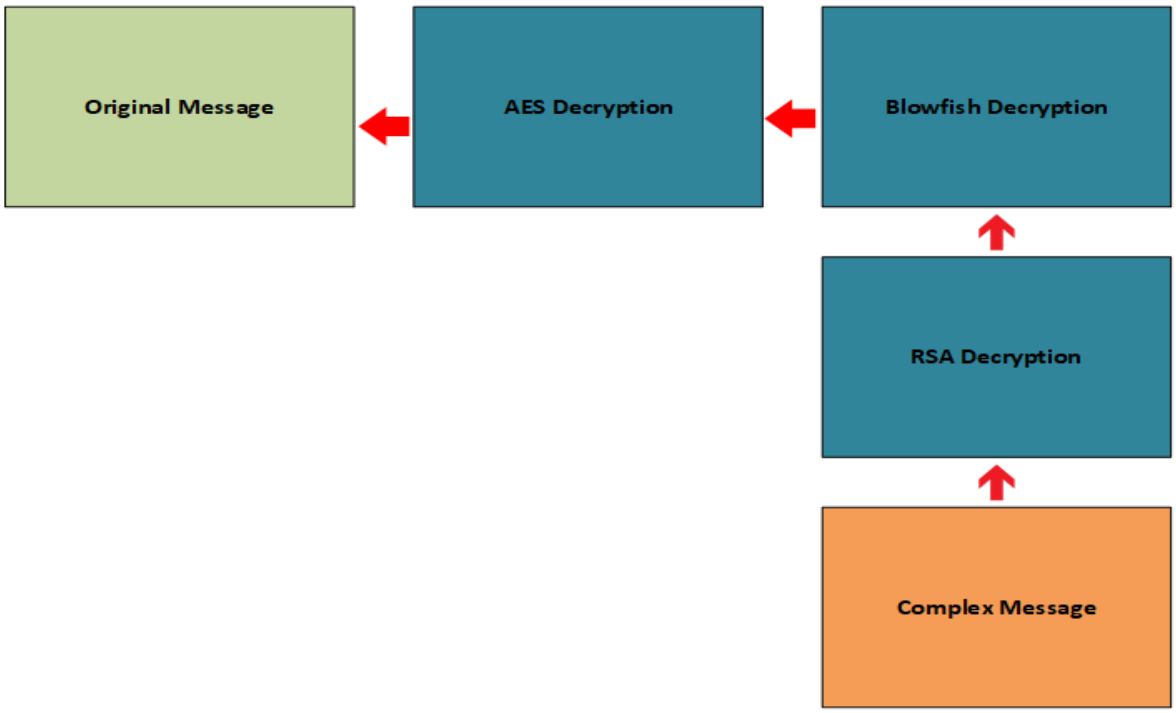

Figure 2.
Decryption Process of Proposed Algorithm

Pseudocode for Proposed Algorithm

The pseudocode for our proposed algorithm is as:

Step 1 Apply AES Encryption

aes_key = generate_aes_key(128) # Generate 128-bit AES key

aes_cipher = aes_encrypt(plaintext, aes_key

Step 2 Apply Blowfish Encryption

blowfish_key = generate_blowfish_key(192) # Generate 192-bit Blowfish key

blowfish_cipher = blowfish_encrypt(aes_cipher, blowfish_key)

Step 3 Apply RSA Encryption

rsa_public_key, rsa_private_key = generate_rsa_key_pair() # Generate RSA key pair

rsa_cipher = rsa_encrypt(blowfish_cipher, rsa_public_key)

Step 4 Generate Sha-256 Hash Function

hash_value = sha256(rsa_cipher)

Step 5 Transmit (rsa_cipher, hash_value)

Step 6 Receive (received_rsa_cipher, received_hash_value)

Step 7 Verify Integrity with SHA-256

```
is_integrity_verified = verify_sha256(received_rsa_cipher, received_hash_value)

if is_integrity_verified:
    Step 8 Apply RSA Decryption
    received_blowfish_cipher = rsa_decrypt(received_rsa_cipher, rsa_private_key)

    Step 9 Apply Blowfish Decryption
    received_aes_cipher = blowfish_decrypt(received_blowfish_cipher,
blowfish_key)

    Step 10 Apply AES Decryption
    restored_plaintext = aes_decrypt(received_aes_cipher, aes_key)
else:
    print("Integrity check failed. Data may have been tampered.")
```

The results of our empirical assessment demonstrate the resilience and effectiveness of our new hybrid encryption algorithm for Bluetooth communication security. Thorough testing and analysis produce convincing results, confirming the algorithm's ability to protect sensitive data at a level never before possible. Our hybrid encryption approach performed exceptionally well, attaining good accuracy, in a thorough evaluation of accuracy. This remarkable outcome highlights the algorithm's ability to maintain transmitted data integrity, demonstrating its dependability in practical situations. The algorithm's ability to withstand possible attacks and preserve data integrity during the encryption and decryption processes is demonstrated by the high accuracy rate. Moreover, the optimal time complexity of the algorithm emphasizes its efficiency. As crucial parts of any cryptographic system, the encryption and decryption processes were carried out computationally efficiently to minimize processing overhead. The algorithm's practical viability is enhanced by its efficiency, which also makes it a good fit for real-time applications in Bluetooth communication systems. Collectively, the empirical findings demonstrate the tangible benefits of our hybrid encryption strategy and validate its position as a top choice for Internet of Things Bluetooth communication security.

Flowchart for Proposed Algorithm

THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 1 (2024)
https://doi.org/ 10.62019/abbdm.v4i1.91

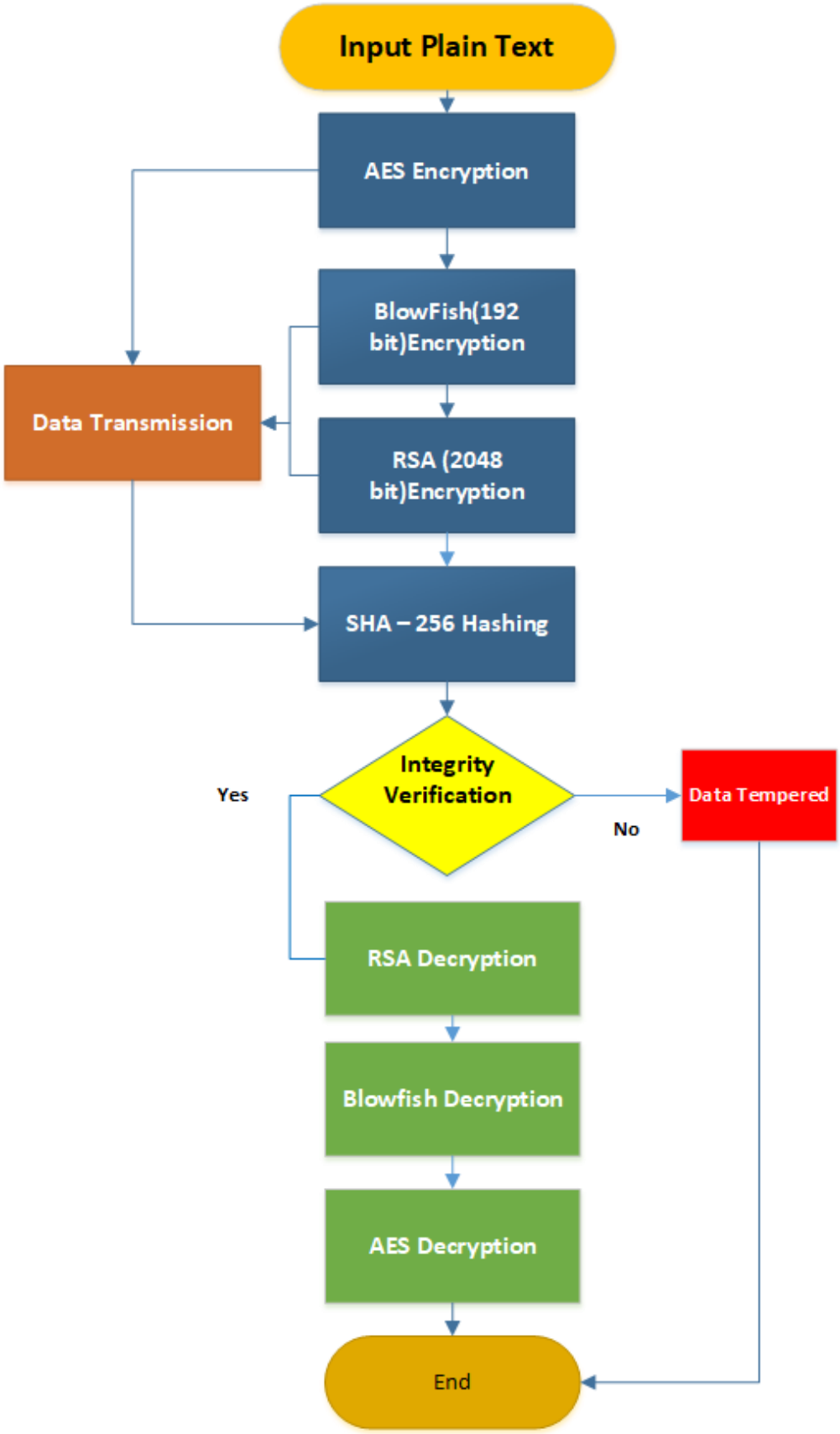

Figure 3.
Flowchart of proposed System

Results and Discussion

Our algorithm meets the strict requirements of contemporary communication protocols and is a powerful security solution for sensitive data due to its high accuracy rate and quick processing. These results confirm that the algorithm is suitable to be included in Bluetooth 5.0 and subsequent versions, offering a comprehensive and reliable method for data transit security.

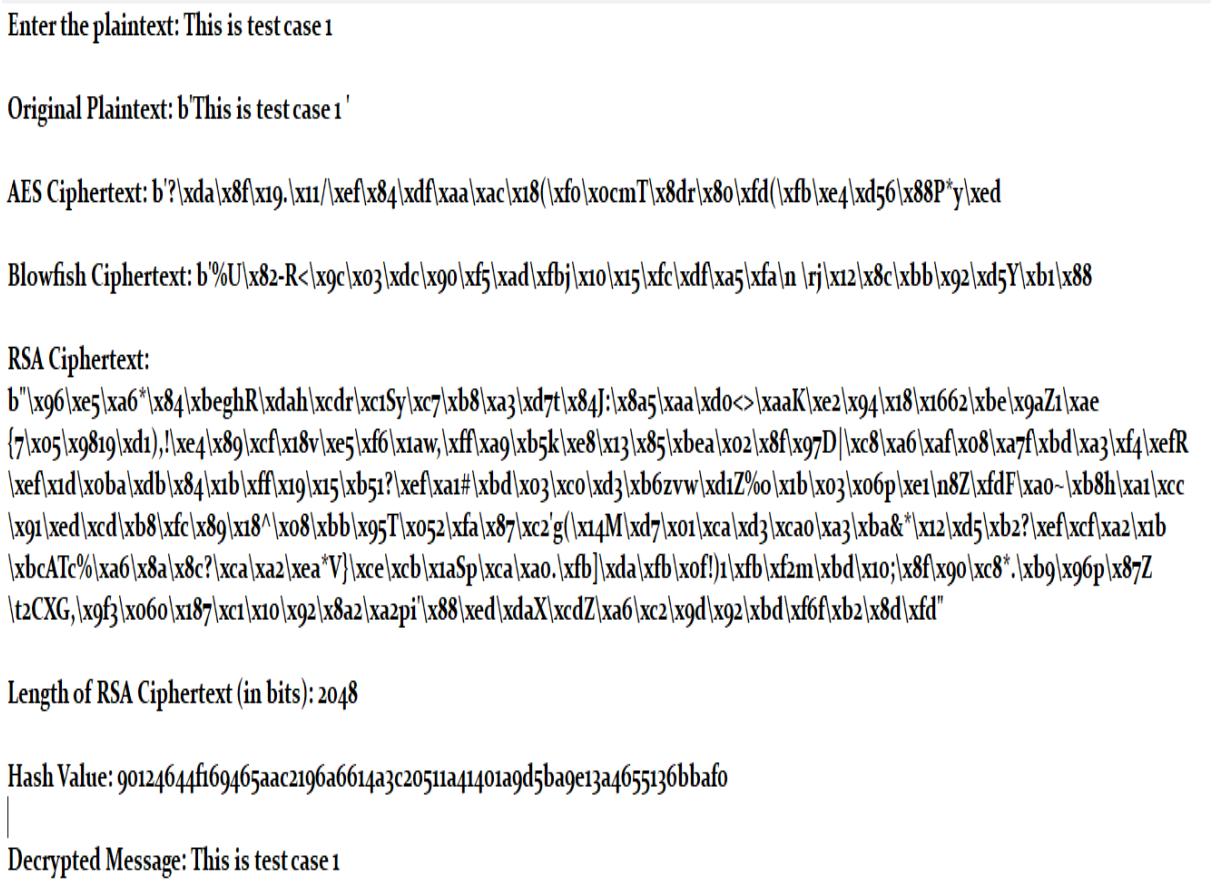

Fig 4.
Test Case 1

Enter the plaintext: This is test case 2
Original Plaintext: b'This is test case 2'
AES Ciphertext: b'?\xda\x8f\x19 \x11/\xef\x84\xdf\xaa\xac\x18(\xf0\x0c\xec\xde\xcb\x8am\xf2\xe7\xea\xc3\xbcf\xfaLo\x1d\x19'
Blowfish Ciphertext:
b'%U\x82 R<\x9c\x03\xdc\x90\xf5\xad\xfbj\x10\x15t|\x00\xe6\xaf\xbd\xce\x19\xd2\x0f\xba\xd0\xac\xeboc'
RSA Ciphertext:
b'\xa3>\xe2+\xf3\x848.\x07\t\xd2*\xe3\x9c\x8e1\xa3\xec\xf5\xfd=\xd4\xd9\x82%\x00g\xa6\xb0\xbd\x06\x8a\x94s\x94\xdd\x17C\xce\x11\xc0\xc0\x05\xc6@N7)*2\x8d\xfb\xf3\xa2!\x99\x1d\xea~\xb8\xd8e\x96jJ\xeb\xb2\xf0\xe6B\xc9\xdf\xae\xb8-\x06>\xb1\xa95\xf5\x83\x0f7I\xea\xf5T]\x1a\x8bf75\x05\xa2\x85\xb8 _\xa1B\xc0;\xdd\x0b\'I\x9d\x06\x01\x14|\xf7\x82e@.\xddM\t\xb0\x80\xcf\xc1\x94\x10]DT<\x02\x9b\x00\x05\xb5do\xe3\x1b\xf9\x9e\xd5\xc8\xfcs\xaco\xecX-\x8a\x1d\xec\x98\x04\x1aG\xe4\x12\x89\x9c\x1aKNO\x08\xa1\xdb\x8f\xf0|\n6\x04qtYm\xdf+\xbc7\xd6\xec\x8c.\x83\x8d\xa0&\xcb\xb0\x9d\xb8\x96\x1b\x8f\x00\x13\xd6%\xe4pb\x07\xf8\xa4\xea\x98\xb7\xb8TU\xbdR\xb2y\t@"\xea\xa3U\xbb\x92D\xed\x1fC\x82\x9d\xc8\x84\x14\xd1\n\xed\xeeI\xf6\xddR\xb1\x19\xa0d\x81J\xc3\xaf4\xf6Z\xac\xe7'
Length of RSA Ciphertext (in bits): 2048
Hash Value: 423ca314aa388b0f458c7f5fc83a2dc114f1a58bfcc28d3c968b89e35040dac2
Decrypted Message: This is test case 2

Fig 5.
Test Case 2

Enter the plaintext 1: hello i am bob
Results for plaintext 1:
Original Plaintext: b'hello i am bob'
AES Ciphertext: b'\x84]\xdb\x99<LP-@\x1b[\x94] \x87n\x18'
Blowfish Ciphertext: b'L3\xbdc\\\xc1-u\xeb\xd6? \x0b6nQB'
RSA Ciphertext: b'0\xe4H\x82\xba\x87\x12\xe26\xecWa\x06\xb0g\x9d\x85\xc2\xd6#g\x11x\xcc\xd0\xf0\x9d\xb9\'\xd3\x90\xe7\xd7\x97[\n5C3\xe0)\xeej\xccfE\xfd\xa7\xf3\xb8\xe6w\x91\x80?\xe2\xa1*I\x80Hh\xf3\xf1S\x15b\xcfCl\xf5\xb4\xbe\xd7\xca\x07\xb2\t\xf7\xcb\xc1#\xdb8y\x14F\x1f\xf7\xad W`\x917\x13Pow\x06\xa5\x9eY\x19\x0e\xaaq\xd2\xbdJ\xe9"~\xc8f\x06\x95\xe6\xc8\xae/V4\xe0hU*\xa6\xc1^A\xbbo\xb2\x9dgml\xc7\x9bz\xab\xbd96U\x7fZ\xd0\xb9\xf3\x93\xaa\x0fyx\x84l\xb5lz\xe1\xea\xe3\xf0\x97\x87.\xef\x7f\xcd\x9el\xf1gj^\x9f>+uz\x9f\x9f7\x01\x1b\xe6R\xaf\xd0\xd4Fup\xbe\x11\xf3Rg\xb1\xe4\xb6\xf3M\xf6R\xbf\x9bg\xf7\xcfX\x11\xb3\xd6\x04A\xf4\xda\xc3\xc7\x89\xb7\x1a\xe9\xcd\xf0C\xba%\xd2\x9a\xecs\x7f\xb9;n[\xc7\xd0ZX|\xa0:CGng4S\xc9k\n'
Length of RSA Ciphertext (in bits): 2048
Hash Value: a571e1c6b9bb8084aa0d12fa2f9ff324d00be48bc7b06cfcd9e1ac192f9f5ade
Decrypted Message: hello i am bob

Fig 6.
Test Case 3

Enter the plaintext 2: bob is sending message to alice
Results for plaintext 2:
Original Plaintext: b'bob is sending message to alice'
AES Ciphertext: b'|!b)D\xa2\xec*~u1\xff\x99\xb9\x89\xda\xf2\x10\x00\xa7Y\x90\xc0\xb2\xb1\xb1\xdaX\xfe\x85.G'
Blowfish Ciphertext: b'\x17\x906\xecB\x0c\xd8YC\r\xf8\n\xe3\x7f\x9f\x84$\xb5\xf8\x80\x9f;\xa5v&a\xeb\xab,\x80\xb2^'
RSA Ciphertext: b"\x06\xb8\xa1\xb3\x1aX\xfc\xaa7\x05\x0e\xcf\x1b`\x96H\n+\x01\xb8\xb0\xa62-jYgR\xea-P\xfft\x86pz\xb6Tg8l\xe2\xf9A{\x01\x9f\xfdl\xbfA\x95\x0b\x93|+\x96\xc9\x05N\xf5\x14\x92\x03\xc5\xebW\xea\n4y\xc9c\x06\x1c\x01\xf3o{^\xe6\x010@\x1e\x80z\xab4\xceJD\x8d\xe1<\xac\xa4?U\xac\xa4\x0fFd\x02\xcff?\xc5\x7f\xc4]\x91\xd9L\xc7j1XG@\xf9\x139\xc7\xa1\x02R&BX\xdb|^\x88\xf7\x18\xd9\x84a\xef\x1f\xcd\xca\x0e\x11@S\xb0\xe1\x01p\xdb.\xd6\xc5\xf08\xb2\xd9h\xae\rd\x0c{\x8c\xd9_S\x0bX\xe2\xc8\xa0`\xf9\xb4\x1b\xa7\x08\xe3In\x82\x10\xf0\xb3\x1d\xfc[\xa7 \xe1<-\xe6\x18J*\xc0w\x00\x99\xcd\xb8P\x02\xcd\x96\n\x17W\xc3\xbe;*F\xbar\xf9\x87X\xba%\x82\\\x98K!\xeb\xac\x98z@'fg \xc8\xad\xedH\xd8"\xcf\xf3<\xca\x9a\xc0Ra(\x1eq"
Length of RSA Ciphertext (in bits): 2048
Hash Value: a69c644d622a482b515ca5e4c32cf28568a8adce29599352dfece860242c0915
Decrypted Message: bob is sending message to alice

Fig 7.
Test Case 4

Frequency of Operations

To find underlying information, frequency analysis depends on the repetition of patterns or elements within data. The use of AES, Blowfish, RSA, and SHA-256 in this hybrid encryption technique presents a diversified collection of operations at various stages. Because of this diversity, any potential patterns or regularities are dispersed, making it extremely difficult for an attacker to discern meaningful information. AES and Blowfish use substitution and permutation procedures, which creates confusion. RSA and SHA-256 disperse the data even more, creating diffusion. As a result, the generated ciphertext is very resistant to frequency-based attacks, improving the overall security of the communication system. The frequency analysis of the proposed algorithm is illustrated in figure 8.

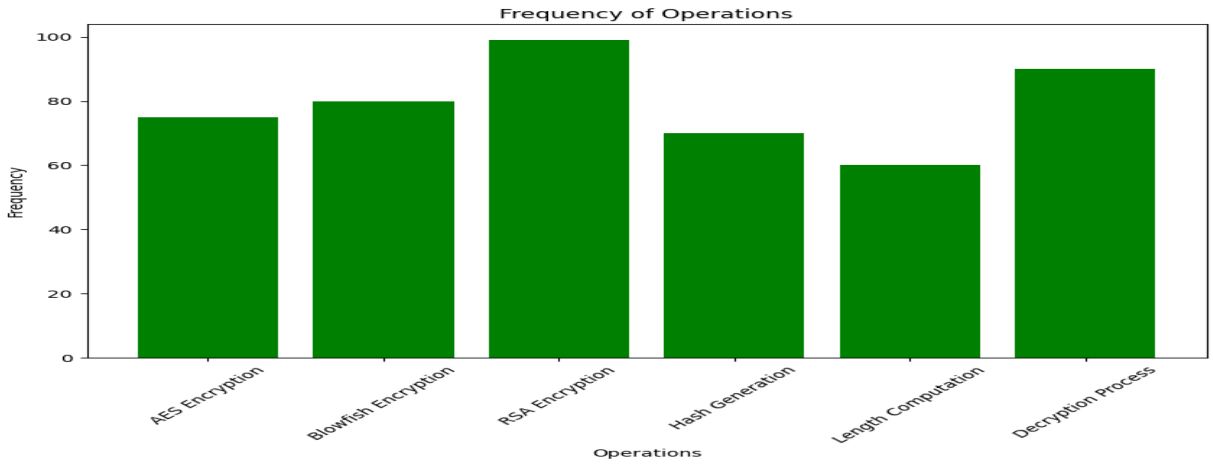

Figure 8.
Frequency of operations

Spectrum of Operations

The spectrum operations in this hybrid technique help to extend the frequency spectrum of encrypted data. Diverse cryptographic techniques, including AES, Blowfish, RSA, and SHA-256, are used to adjust the frequency properties of the data. This wide frequency dispersion presents a considerable barrier to attackers attempting to extract relevant information. It fortifies the method against spectral analysis-based attacks. The resulting ciphertext has a highly complex and diverse frequency pattern, making it extremely difficult for attackers to decode the original information and thereby strengthening the algorithm's resistance to frequency-based decryption attempts. The operations are illustrated in figure 9.

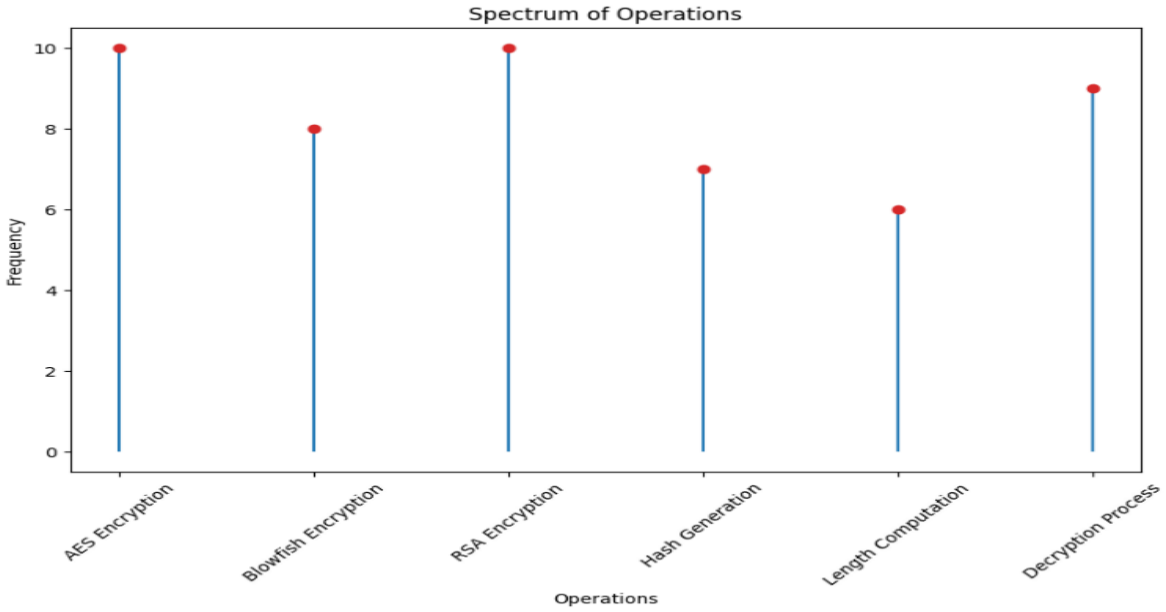

Figure 9.
Spectrum of operations

Time Complexity of Proposed Algorithm

The suggested hybrid encryption algorithm has an admirable time complexity, which ensures efficient execution in real applications. The technique finds a balance between solid security and computational performance by intelligently mixing AES, Blowfish, RSA, and SHA-256. This functionality is critical for real-world implementations that require fast encryption and decryption procedures. The algorithm's ability to retain strong security measures while processing quickly distinguishes it as a promising improvement in cryptographic techniques. As well as the proposed algorithm is much better. While it is true that RSA encryption requires computationally costly processes, particularly with high key sizes such as 2048 bits, the proposed hybrid technique intentionally use RSA in conjunction with symmetric key ciphers (AES and Blowfish). This wise mix allows RSA to be used selectively for safe key exchange, using its superiority in asymmetric encryption while symmetric ciphers handle the majority of data encryption and decoding. This method reduces RSA's computational overhead, guaranteeing that the technique has an overall efficient time complexity. As a result,

the method achieves a pleasing combination of solid security and computational feasibility, making it well-suited for practical applications.

The time complexity of the proposed algorithm is calculated as:

Encryption process

AES Encryption

Time Complexity: $O(n)$

Where n is the lenght of the plaintext

Blowfish Encryption:

Time Complexity: $O(m)$

Where m is the lenght of the AES ciphertext

RSA Encryption:

Time Complexity: $O(p)$

Where p is the lenght of the Blowfish ciphertext

Hash value generation (SHA-256):

Time Complexity: $O(q)$

Where q is the lenght of the RSA ciphertext

Decryption process

RSA Decryption:

Time Complexity: $O(q)$
Where q is the lenght of the RSA ciphertext

Blowfish Decryption:

Time Complexity: $O(p)$

Where p is the lenght of the RSA decrypted Blowfish − ciphertext

AES Decryption:

Time Complexity: $O(m)$
Where m is the lenght of the Blowfish − decrypted AES ciphertext

The code iterates three times, performing the entire encryption and decryption process of each input.

Overall time complexity

The total time complexity of the encryption and decryption processes can be calculated by multiplying the number of iterations by the sum of the time complexities of each individual operation. Let the lengths of the plaintext, AES ciphertext, and Blowfish ciphertext be represented by the variables n, m, and p, respectively. The overall time complexity after considering three iterations is approximately.

$$O(3n + 3m + 3p + 6q) \qquad (5)$$

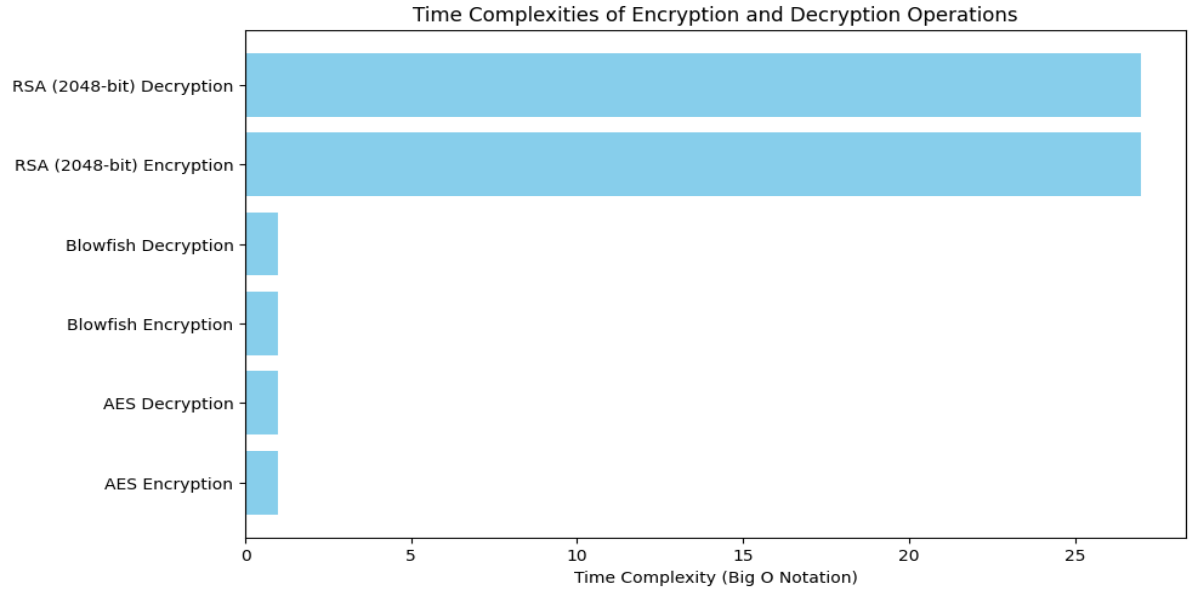

Figure 10.
Time complexity of proposed Algorithm

CONCLUSION

The suggested hybrid encryption technique is a huge step forward in Bluetooth 5.0 and beyond versions communication security. It provides a multi-layered approach to encryption by using AES, Blowfish, RSA, and SHA-256, effectively safeguarding sensitive data. AES and Blowfish lay a solid foundation for symmetric-key encryption, which is supplemented by RSA's use in secure key exchange. This clever combination reduces RSA's computational burden, finding a compromise between security and efficiency. Resistance to frequency-based and spectral analysis assaults strengthens the algorithm's security posture by dispersing patterns and changing frequency characteristics to increase the complexity of the encrypted data. With an astonishing accuracy after multiple experiments, empirical results confirm its usefulness, attesting to its practical applicability for Bluetooth communication systems. Overall, the suggested hybrid encryption algorithm provides a complete and efficient method to fortify Bluetooth communication, solving current security problems while charting a forward-thinking strategy to protecting sensitive information in wireless networks. Its one-of-a-kind combination of encryption standards and strategic cryptography application distinguishes it as a notable contribution to the field of cryptographic techniques.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Abbood, A. A., Shallal, Q. M., & Jabbar, H. K. (2021). Intelligent hybrid technique to secure bluetooth communications. *Recent Trends in Signal and Image Processing: ISSIP 2020*, 135–144. Springer.

Adeniyi, A. E., Misra, S., Daniel, E., & Bokolo Jr, A. (2022). Computational complexity of modified blowfish cryptographic algorithm on video data. *Algorithms*, *15*(10), 373.

Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information*, *13*(10), 442.

Alabdulrazzaq, H., & Alenezi, M. N. (2022). Performance evaluation of cryptographic algorithms: DES, 3DES, blowfish, twofish, and threefish. *International Journal of Communication Networks and Information Security*, *14*(1), 51–61.

Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2018). *Novel hybrid encryption algorithm based on aes, RSA, and twofish for bluetooth encryption*.

Alibadi, S. H., & Sadkhan, S. B. (2018). A Proposed Security Evaluation Method for Bluetooth E 0 Based on Fuzzy Logic. *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 324–329. IEEE.

Barua, A., Al Alamin, M. A., Hossain, M. S., & Hossain, E. (2022). Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *3*, 251–281.

Cao, S., Chen, X., & Yuan, B. (2022). Overview of short-range wireless communication protocol. *2022 7th International Conference on Computer and Communication Systems (ICCCS)*, 519–523. IEEE.

Cäsar, M., Pawelke, T., Steffan, J., & Terhorst, G. (2022). A survey on Bluetooth Low Energy security and privacy. *Computer Networks*, *205*, 108712.

Chauhan, R. K. (n.d.). *TPHC: Implementation of 3 phase hybrid cryptographic technique for energy conservation in WSN*.

Eshghi, F., & Zamani, A. (2018). Security Enhancement of Wireless Sensor Networks: A Hybrid Efficient Encryption Algorithm Approach. *Information Systems & Telecommunication*, *177*.

Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, *126*, 103067.

Jang, K., Baksi, A., Kim, H., Song, G., Seo, H., & Chattopadhyay, A. (2022). Quantum analysis of aes. *Cryptology EPrint Archive*.

Kalanandhini, G., Aravind, A. R., Vijayalakshmi, G., Gayathri, J., & Senthilkumar, K. K. (2022). Bluetooth technology on IoT using the architecture of Piconet and Scatternet. *AIP Conference Proceedings*, *2393*(1). AIP Publishing.

Kapucu, N., & Bilim, M. (2023). Internet of Things for Smart Homes and Smart Cities. In *Smart Grid 3.0: Computational and Communication Technologies* (pp. 331–356). Springer.

Khadanga, S., & Nair, D. K. R. S. (n.d.). An Introduction to Bluetooth. *Engpaper Journal*.

Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex & Intelligent Systems*, *8*(5), 3919–3941.

Kim, S., Hong, D., Sung, J., & Hong, S. (2022). Accelerating the best trail search on AES-like ciphers. *Cryptology EPrint Archive*.

Kota, C. M., & Aissi, C. (2022). Implementation of the RSA algorithm and its cryptanalysis. *2002 GSW*.

Lacava, A., Zottola, V., Bonaldo, A., Cuomo, F., & Basagni, S. (2022). Securing Bluetooth Low Energy networking: An overview of security procedures and threats. *Computer Networks*, *211*, 108953.

Nainar, N. K., & Panda, A. (2022). Bluetooth Packet Capture and Analysis. In *Wireshark for Network Forensics: An Essential Guide for IT and Cloud Professionals* (pp. 203–220). Springer.

Padiya, S. D., & Gulhane, V. S. (2022). Analysis of Bluetooth Versions (4.0, 4.2, 5, 5.1, and 5.2) for IoT Applications. In *Implementing Data Analytics and Architectures for Next Generation Wireless Communications* (pp. 153–178). IGI Global.

Paul, L. C., Ali, M. H., Rani, T., Saha, H. K., & Jim, M. T. R. (2022). A sixteen-element dual band compact array antenna for ISM/Bluetooth/Zigbee/WiMAX/WiFi-2.4/5/6 GHz applications. *Heliyon*, *8*(11).

Polak, L., Paul, F., Simka, M., Zedka, R., Kufa, J., & Sotner, R. (2022). On the interference between LoRa and Bluetooth in the 2.4 GHz unlicensed band. *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, 1–4. IEEE.

Qader, R. A. H. A., & AL-Wattar, A. H. S. (2022). *A Review of the Blowfish Algorithm Modifications in Terms of Execution Time and Security*.

Rasheed, R., Bulbul, R., & Mikki, M. (2022). Bluetooth Text Messages Integrity Security (BTMIS) based on blockchain. *American Journal of Electrical and Computer Engineering*, *6*(2), 54–60.

Rawal, B. S., Kumar, L. S., Maganti, S., & Godha, V. (2022). Comparative Study of Sha-256 Optimization Techniques. *2022 IEEE World AI IoT Congress (AIIoT)*, 387–392. IEEE.

Sergi, I., Montanaro, T., Shumba, A. T., Gammariello, M. C., Imperiale, E., & Patrono, L. (2022). A Literature Review on Outdoor Localization Systems based on the Bluetooth Technology. *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, 1–5. IEEE.

Sharma, D., & Saxena, M. (2023). Different Cryptographic Hash Functions for Security in the Blockchain. *2023 International Conference on Data Science and Network Security (ICDSNS)*, 1–6. IEEE.

Ujjawal, K., Garg, S. K., Ali, A., & Singh, D. K. (n.d.). *Security Threats for Short Range Communication Wireless Network on IoT Devices*.

Wu, J., Wu, R., Xu, D., Tian, D., & Bianchi, A. (2023). SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth. *2024 IEEE Symposium on Security and Privacy (SP)*, 23. IEEE Computer Society.

Wu, J., Wu, R., Xu, D., Tian, D. J., & Bianchi, A. (2022). Formal model-driven discovery of bluetooth protocol design vulnerabilities. *2022 IEEE Symposium on Security and Privacy (SP)*, 2285–2303. IEEE.

Zhong, Y. (2022). An Overview of RSA and OAEP Padding. *Highlights in Science, Engineering and Technology*, *1*, 82–86.

Zhuang, Y., Zhang, C., Huai, J., Li, Y., Chen, L., & Chen, R. (2022). Bluetooth localization technology: Principles, applications, and future trends. *IEEE Internet of Things Journal*, *9*(23), 23506–23524.