Development of a Model for Preventing Information Leakage

Isaac Akinduro
Federal University of Technology, Akure, Ondo State, Nigeria.

Isaac Afolabi
Federal University of Technology, Akure, Ondo State, Nigeria.

Otasowie Owolafe
Federal University of Technology, Akure, Ondo State, Nigeria

doi: https://doi.org/10.37745/ejcsit.2013/vol13n163449 Published May 09, 2025

Citation: Akinduro I., Afolabi I. and Owolafe O. (2025) Development of a Model for Preventing Information Leakage, *European Journal of Computer Science and Information Technology*,13(16),34-49

Abstract: *The increase in the use of the internet around the world provided easier way of communication and information sharing that has led to the huge challenge of data leakage on the network. In an academic environment such as higher institutions of learning, the need to ensure that access to data and sensitive information are given to authorized users become imperative. However, this is not always the case as security bridges are often experienced. This study proposed an RSA public key encryption algorithm, to prevent information leakage. The system developed RSA public key encryption algorithm, thus provided the required security mechanism that prevents information leakage in a public environment.*

Keywords: information leakage, RSA, public encryption, algorithm

INTRODUCTION

In today's digital era, information leakage is a critical concern for individuals, organizations, and governments. Unauthorized disclosure of sensitive data can result in financial losses, reputational damage, and privacy breaches. This research proposes a novel model that integrates multiple strategies to mitigate the risk of information leakage.

With increasing reliance on technology and data sharing, various vulnerabilities arise. [1] highlight risks in third-party cloud computing, while [2] discuss potential leaks in collaborative deep learning. These challenges emphasize the urgency of developing robust preventive models.

Privacy preservation is essential in mitigating indirect leaks in collaborative learning [3]. Secure communication through quantum dialogue [4] can enhance confidentiality, leveraging quantum entanglement for secure exchanges. Additionally, blockchain technology provides accountability by maintaining immutable records, reducing leakage risks [5].

A comprehensive information-leakage-resilience framework, integrating policies, technological controls, and user awareness, strengthens security [6] However, risks persist in embedding models used in machine learning, necessitating additional safeguards [7].

Given the widespread use of deep neural networks, machine learning, and hardware-oriented security, developing effective leakage-prevention models is more crucial than ever. By combining advanced technologies and organizational strategies, this research aims to enhance data security across various domains.

Past research has struggled to prevent information leakage from zero-day vulnerabilities and novel attacks. Recent breaches in real-time systems highlight the need to integrate security as a fundamental design principle. Information leakage occurs across multiple platforms, yet existing research lacks comprehensive cross-platform solutions for mobile devices, cloud services, and traditional networks. Additionally, many security models face usability challenges, emphasizing the need for user-friendly prevention models with minimal false positives.

A robust defense against information leakage requires combining multiple techniques. Machine learning models, such as clustering, decision trees, and neural networks, help detect unusual data access patterns indicative of leakage. Encryption algorithms like AES ensure data protection at rest and in transit. Access control models including role-based, attribute-based, and mandatory access control restrict unauthorized access to sensitive information.

Data Loss Prevention (DLP) systems enhance security by monitoring data in motion, at rest, and in use, enforcing policies to prevent leakage. Adapting these methods to evolving threats is crucial for effective information security.

The objective of this project is to develop an information leakage prevention model utilizing the RSA Public Encryption algorithm. This model aims to enhance data security by ensuring that sensitive information remains protected from unauthorized access and leakage. By leveraging RSA encryption, the project seeks to provide a robust mechanism for securing data both at rest and in transit.

Additionally, the project will evaluate the performance of the developed model to assess its effectiveness in preventing information leakage. This evaluation will involve analyzing key security metrics such as encryption efficiency, computational overhead, and resistance to potential attacks. The findings will help determine the model's reliability and suitability for real-world applications, ensuring that it meets the necessary security and usability standards.

LITERATURE REVIEW

[8] conducted research on information leakage between FPGA long wires. Their study highlighted the vulnerability of long wires in FPGA architectures to information leakage, which can be exploited by adversaries to gain unauthorized access to sensitive data. This finding underscores the need for robust approaches to prevent information leakage in electronic systems.

Another study by [9] demonstrated electromagnetic information leakage from modern processor-memory systems. They highlighted the need for effective countermeasures to mitigate the risk of information leakage in such systems. In the domain of quantum communication, preventing information leakage is crucial to ensure the confidentiality and integrity of transmitted data.

[10] focused on information leakage in efficient bidirectional quantum secure direct communication. They highlighted the challenges associated with information leakage in quantum communication protocols and proposed countermeasures to enhance the security of the communication process.

[11] addressed the information leakage problem in high-capacity quantum secure communication with authentication using Einstein-Podolsky-Rosen pairs. Their study emphasized the need for robust authentication mechanisms to prevent information leakage in quantum communication systems.

Cloud computing has gained widespread popularity in recent years, but it also poses significant challenges in terms of information leakage. [12] investigated information leakage in deduplicated storage systems. They demonstrated that deduplication, a commonly used technique in cloud storage, can lead to information leakage if not appropriately implemented. Their findings highlight the importance of implementing robust security measures to prevent information leakage in cloud storage systems.

Machine learning models, although powerful and versatile, are also vulnerable to information leakage. [13] proposed a novel approach to measure data leakage in machine learning models using Fisher information. Their study highlighted the importance of understanding the information leakage risks associated with machine learning algorithms and developing techniques to quantify and mitigate these risks. This research contributes to the development of effective approaches for preventing information leakage in machine learning applications.

In the broader context of information security, [14] discussed data and information leakage prevention. The study highlighted the various techniques and strategies that can be employed to prevent information leakage, such as access control, encryption, data loss prevention, and user awareness training. The research emphasized the need for a comprehensive and multi-faceted approach to prevent information leakage, considering both technical and organizational aspects.

In conclusion, preventing information leakage is a critical concern in various domains, including electronics, quantum communication, cloud computing, and machine learning. Existing models and approaches address the specific challenges associated with information leakage in these domains. The studies discussed in this section highlight the vulnerability of different systems to information leakage and propose countermeasures to prevent unauthorized disclosure of sensitive data. By considering the insights from these studies, researchers can develop a comprehensive model for preventing information leakage that takes into account the unique characteristics and challenges of each domain.

Related Works

According to the data leakage detection system proposed by [15] for improving probability of identifying leakages, in order to detect faulty agent, it made a change in data allocation. The system was able to detect faulty party without tempering integrity of the real data. [16] researched on the significance of data leakage which gave the ideas leading to social network analysis and clustering of text. The work emphasized on different data leakage preventions methods and their related problems. [17] designed a system that makes use of data allocation methods to increase detection of leakages. The robust mail filtering and information leakage system emanated from other applications. The system makes use of fingerprints of messages bodies and email addresses. The research work also emphasized that distributor need to calculate the aspects that make open records corresponding data leakages from various agents.

[18] authored a Fast Detection of Transformed Data Leaks which focused on unpremeditated data leak detection. Detecting various loopholes for the exposure of important data was difficult due to data transformation. In the model designed, two types of sequences where analyzed i.e. sensitive data sequence that requires to be protected from unauthorized parties and content steps which is to be examined for various leaks. The content data may include records extracted from distributed system, or personal computers from supervised network channels. The sensitive data sequences are known to the analysis system. The sensitive data sequences make use of sequence alignment approaches for tracking the patterns in complex data leak which are known to the analysis system. [19] presented an approach to detect data leakages in a very secured communication in any ad-hoc networks. A data provider can own vulnerable data of trusted agents, and some data can be revealed at such permitted place. There was extra security with encryption after the introduction of the fake objects. The system proposed described data loss and reduces performance degradation in a multi-agent environment; it is made up of cryptography and routing protocol execution at each strategic stage during the data transfer. [20] proposed a hybrid detection leakage framework that make use of both signature and anomaly-based solutions thereby leading to both detection and prevention. The system illustrates the

challenges in data loss detection and prevention through a running example within the healthcare domain and presents a framework to address these challenges. The aim of the system is to develop a framework for detection leakage programmed that employs an anomaly-based engine to detect anomalous transactions. The research work fails to show in detail the anomaly-based techniques adopted. [21] presented a work that seeks to explain the objectives and properties of the mobile agents in currently used architecture and platform of mobile world from the currently used approach RPC (Remote Procedure Calling) and new approach RP (Remote Programming) of the mobile network. There was little practical introduction to mobile agent technology and surveys the state of the art in mobile agent research. [21] explained the currently used approach for remote procedure calling and the new approach for remote programming of mobile network. For most mobile agent research, there were little practical introduction to technological application and surveys. [21] proceeds to develop a mobile app using The Aglet mobile-agent Model by gathering of relevant journal articles and categorizing them and describing the fundamental operations of Aglet mobile agent. The result of the research shows that it is purely descriptive.

METHODOLOGY

A conceptual model for Information leakage prevention is proposed using: RSA Public Encryption algorithm which are used to determine the semantic text classification of document and presents an innovative approach to secure communication without information leakage thereby providing accurate document classification. This gives clarity of data which in turn help against leakage in data communication.

This will be considered to ascertain the effectiveness, reliability of the proposed system which will help in making recommendations.

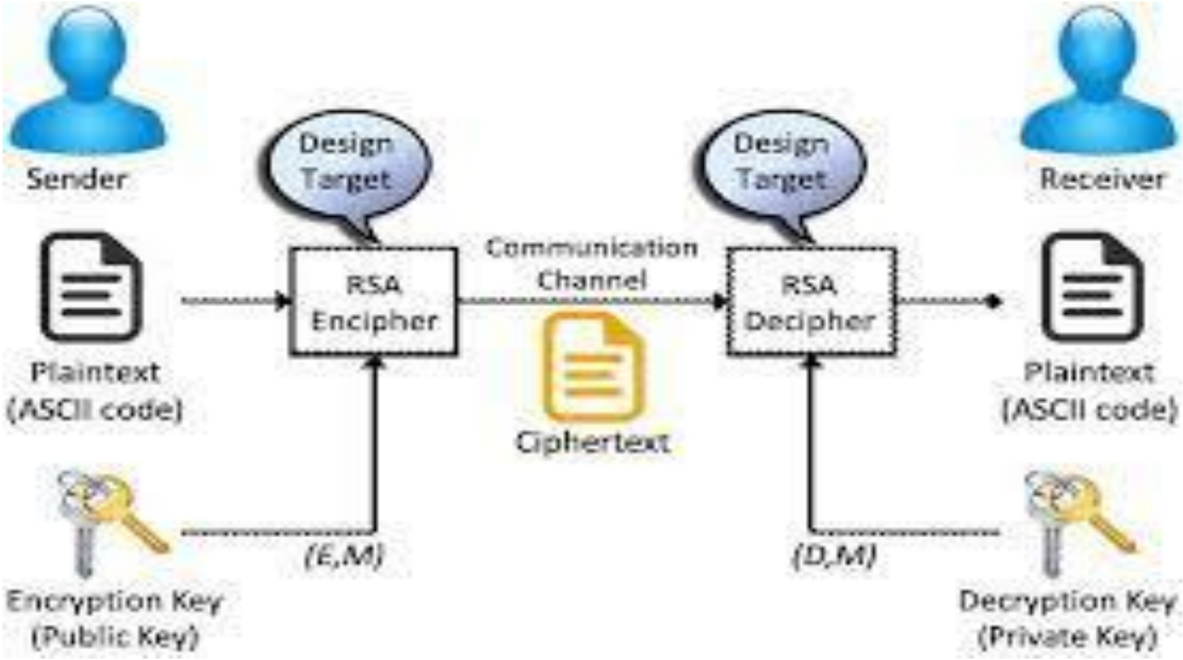
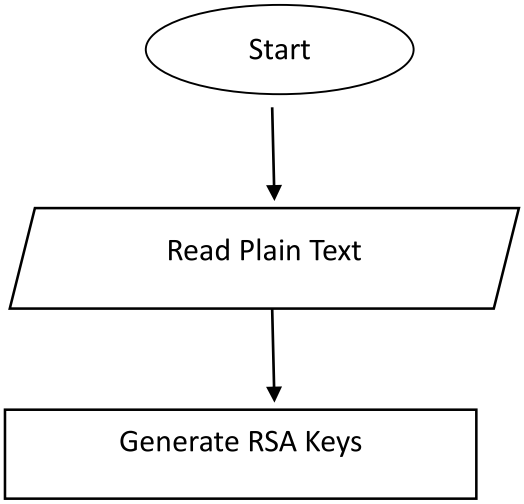


Fig 1: System architecture.

Flow Chart of the Model

A flowchart is the diagrammatic representation of an algorithm, for the proposed model, the flowchart is given below.



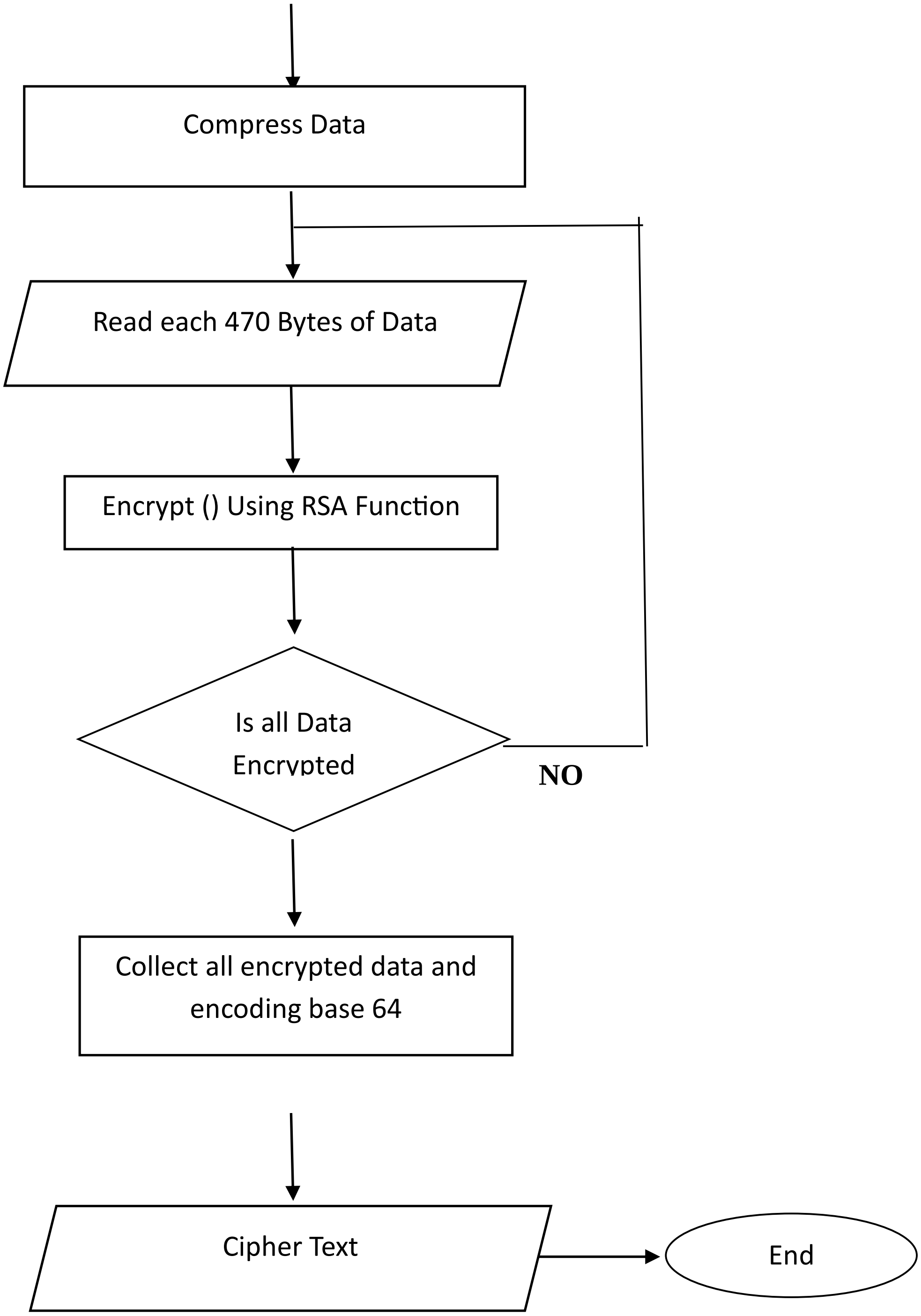

Compress Data
Read each 470 Bytes of Data
Encrypt () Using RSA Function
Is all Data Encrypted
NO
Collect all encrypted data and encoding base 64
Cipher Text
End

Fig 3: Flowchart for Encryption.

The proposed system operates in several stages, beginning with Key Generation. In this step, two large prime numbers, p and q, are selected and used to compute the modulus n = p × q. A public exponent e is chosen, ensuring it is relatively prime to (p-1)(q-1). Then, the private exponent d is calculated as the modular multiplicative inverse of e mod (p-1)(q-1).

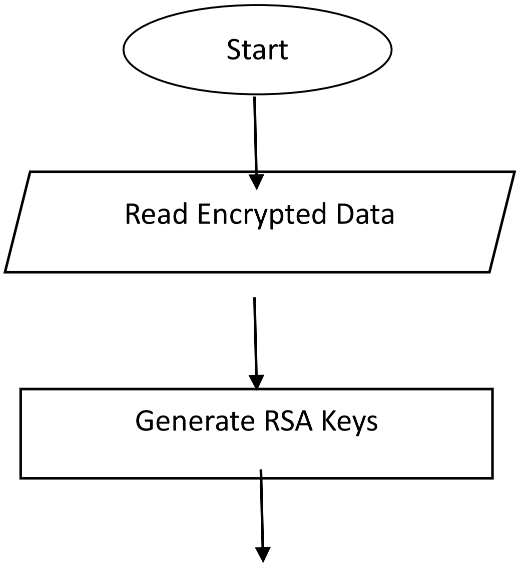
Next, in the Message Preparation phase, the plaintext message is converted into a numerical representation using an appropriate encoding scheme such as ASCII. If necessary, padding is applied to ensure the message is the correct length for encryption.

During Encryption, the plaintext is divided into blocks of suitable length based on the chosen prime numbers. Each block is then encrypted using the formula: ciphertext = plaintext^e mod n.

In the Transmission phase, the encrypted message (ciphertext) is sent to the intended recipient.

The Decryption phase begins when the recipient receives the ciphertext. Each encrypted block is decrypted using the private key d, following the formula: plaintext = ciphertext^d mod n.

Finally, the decrypted blocks are combined to reconstruct the original message, and any applied padding is removed in the Unpadding step, ensuring the final message is accurately restored.



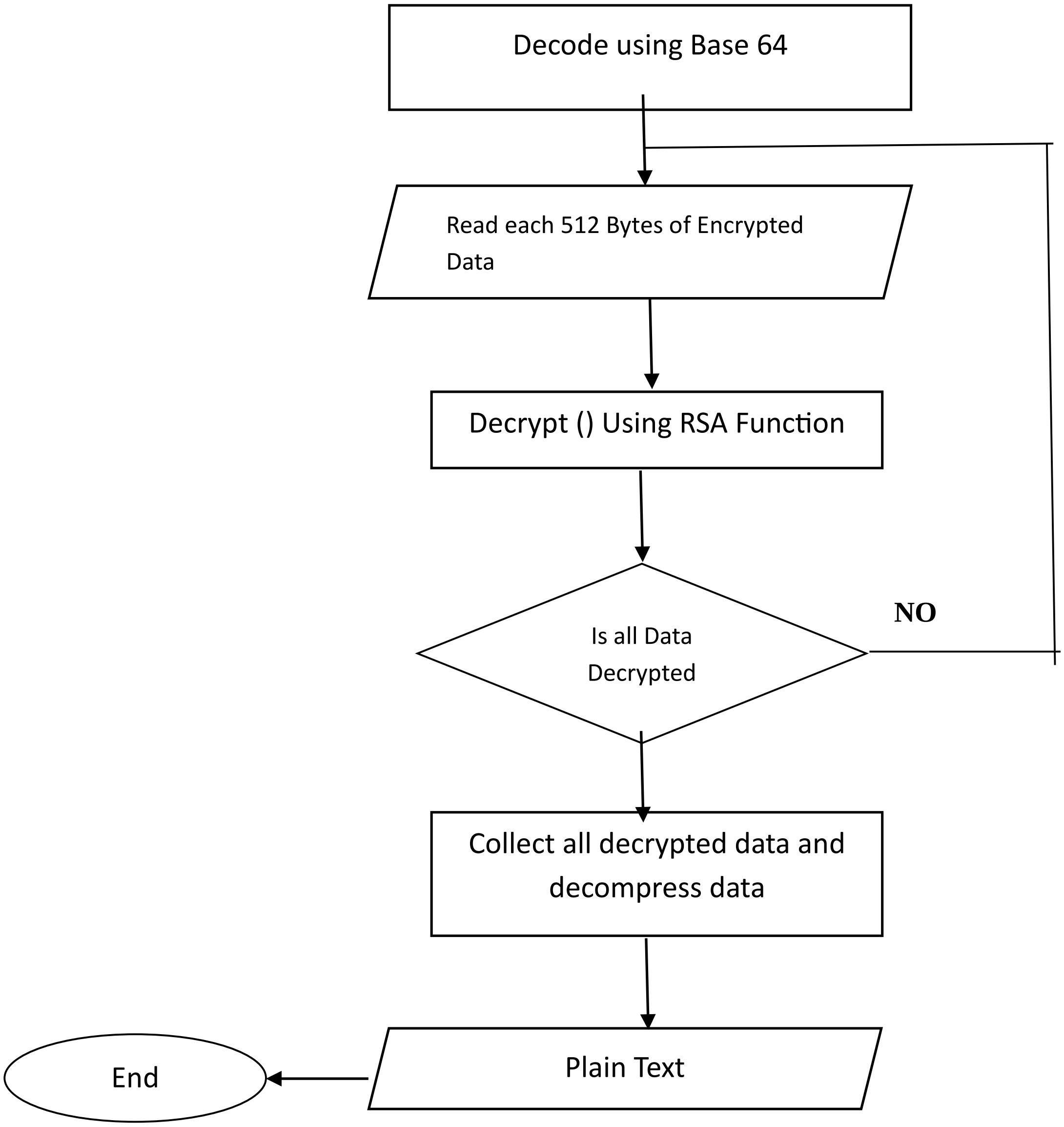

Decode using Base 64
Read each 512 Bytes of Encrypted Data
Decrypt () Using RSA Function
Is all Data Decrypted
NO
Collect all decrypted data and decompress data
Plain Text
End

Fig 3.2: Flowchart for Decryption.

The proposed system operates by first receiving the encrypted message (ciphertext) from the sender. Once received, the system retrieves and verifies the private key (d) associated with the corresponding public key to ensure secure decryption. The ciphertext is then converted into a numerical representation to facilitate processing.

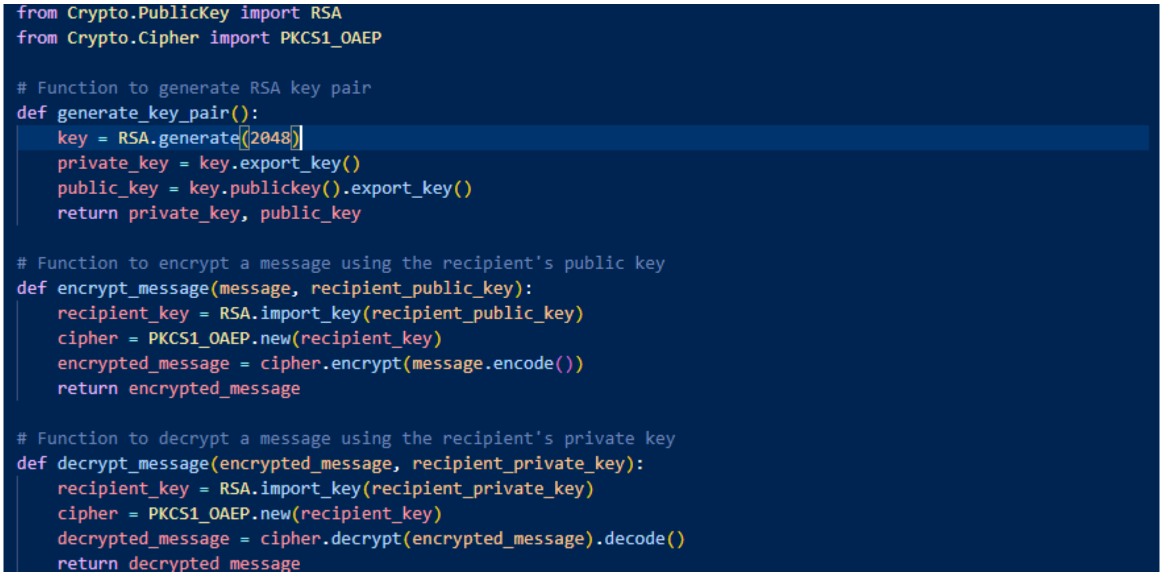
During the decryption phase, each character in the ciphertext undergoes transformation by raising its numerical value to the power of the private exponent (d) modulo the modulus (n), effectively restoring its original numerical value. After this computation, the numerical values are converted back into their respective characters to reconstruct the original plaintext message.

Finally, the decrypted message is made available for viewing and further processing, ensuring that the intended recipient can access and interpret the information securely.

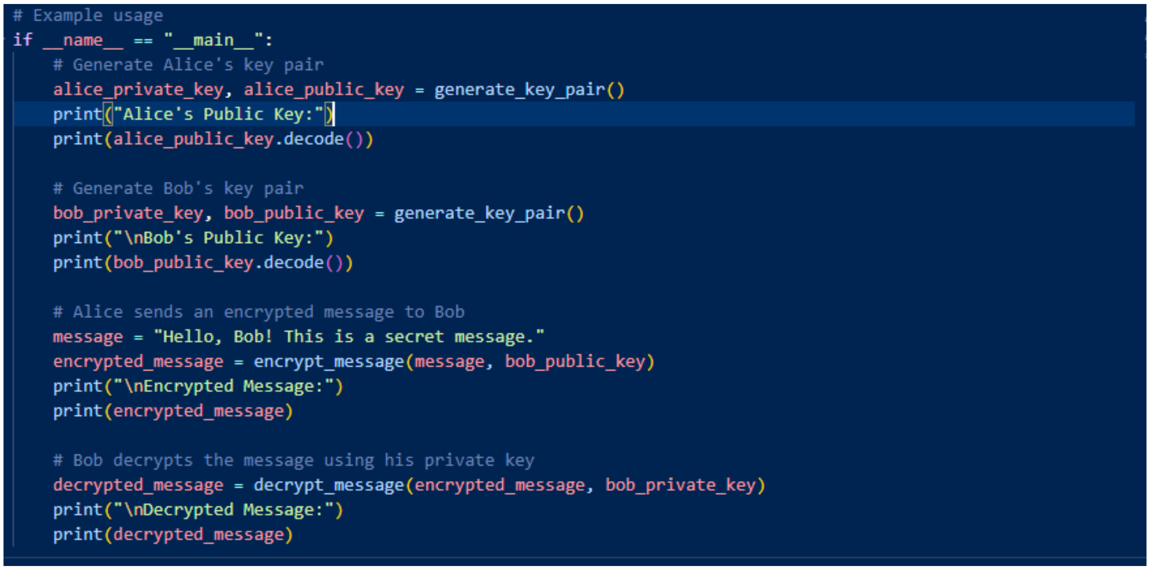
IMPLEMENTATION AND RESULT.

For a system to be valuable, it must be put into practice and verified to ensure that it operates correctly and the model will be thoroughly tested and evaluated for accuracy by comparing the results obtained. This process will help to identify any potential issues or shortcomings in the system, which can then be addressed and resolved to ensure that the final product is of high quality.

RSA Encryption / Decryption using python.

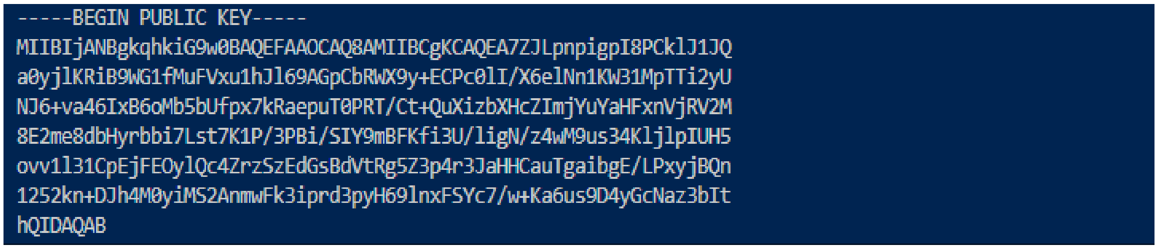


```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

# Function to generate RSA key pair
def generate_key_pair():
    key = RSA.generate(2048)
    private_key = key.export_key()
    public_key = key.publickey().export_key()
    return private_key, public_key

# Function to encrypt a message using the recipient's public key
def encrypt_message(message, recipient_public_key):
    recipient_key = RSA.import_key(recipient_public_key)
    cipher = PKCS1_OAEP.new(recipient_key)
    encrypted_message = cipher.encrypt(message.encode())
    return encrypted_message

# Function to decrypt a message using the recipient's private key
def decrypt_message(encrypted_message, recipient_private_key):
    recipient_key = RSA.import_key(recipient_private_key)
    cipher = PKCS1_OAEP.new(recipient_key)
    decrypted_message = cipher.decrypt(encrypted_message).decode()
    return decrypted_message
```



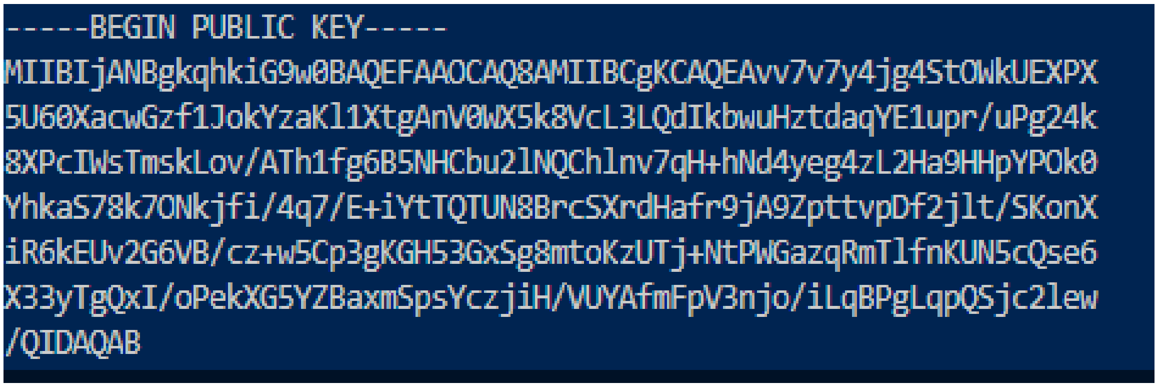
```
# Example usage
if __name__ == "__main__":
    # Generate Alice's key pair
    alice_private_key, alice_public_key = generate_key_pair()
    print("Alice's Public Key:")
    print(alice_public_key.decode())

    # Generate Bob's key pair
    bob_private_key, bob_public_key = generate_key_pair()
    print("\nBob's Public Key:")
    print(bob_public_key.decode())

    # Alice sends an encrypted message to Bob
    message = "Hello, Bob! This is a secret message."
    encrypted_message = encrypt_message(message, bob_public_key)
    print("\nEncrypted Message:")
    print(encrypted_message)

    # Bob decrypts the message using his private key
    decrypted_message = decrypt_message(encrypted_message, bob_private_key)
    print("\nDecrypted Message:")
    print(decrypted_message)
```

Fig 2: Examples



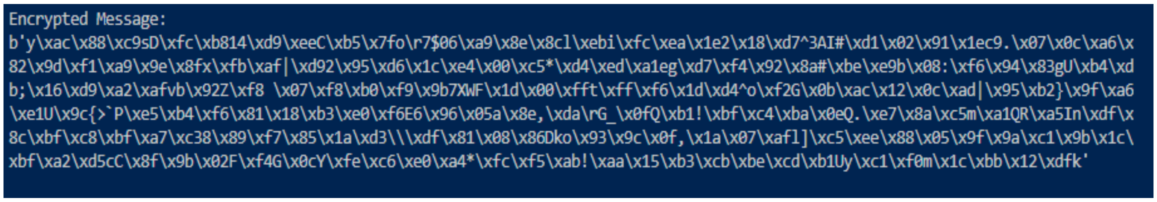
```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7ZJLpnpigpI8PCklJ1JQ
a0yjlKRiB9WG1fMuFVxu1hJl69AGpCbRWX9y+ECPc0lI/X6elNn1KW31MpTTi2yU
NJ6+va46IxB6oMb5bUfpx7kRaepuT0PRT/Ct+QuXizbXHcZImjYuYaHFxnVjRV2M
8E2me8dbHyrbbi7Lst7K1P/3PBi/SIY9mBFKfi3U/ligN/z4wM9us34KljlpIUH5
ovv1l31CpEjFEOylQc4ZrzSzEdGsBdVtRg5Z3p4r3JaHHCauTgaibgE/LPxyjBQn
1252kn+DJh4M0yiMS2AnmwFk3iprd3pyH69lnxFSYc7/w+Ka6us9D4yGcNaz3bIt
hQIDAQAB
```

Fig 3: Alice public key



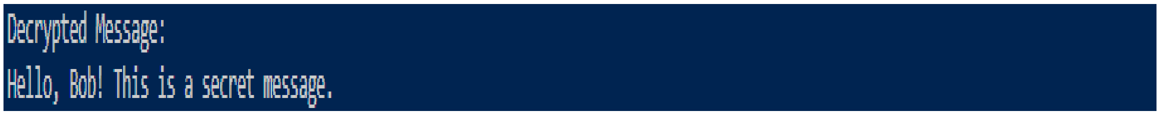
```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvv7v7y4jg4StOWkUEXPX
5U60XacwGzf1JokYzaKl1XtgAnV0WX5k8VcL3LQdIkbwuHztdaqYE1upr/uPg24k
8XPcIWsTmskLov/ATh1fg6B5NHCbu2lNQChlnv7qH+hNd4yeg4zL2Ha9HHpYPOk0
YhkaS78k7ONkjfi/4q7/E+iYtTQTUN8BrcSXrdHafr9jA9ZpttvpDf2jlt/SKonX
iR6kEUv2G6VB/cz+w5Cp3gKGH53GxSg8mtoKzUTj+NtPWGazqRmTlfnKUN5cQse6
X33yTgQxI/oPekXG5YZBaxmSpsYczjiH/VUYAfmFpV3njo/iLqBPgLqpQSjc2lew
/QIDAQAB
```

Fig 4: Bob public key



```
Encrypted Message:
b'y\xac\x88\xc9sD\xfc\xb814\xd9\xeeC\xb5\x7fo\r7$06\xa9\x8e\x8cl\xebi\xfc\xea\x1e2\x18\xd7^3AI#\xd1\x02\x91\x1ec9.\x07\x0c\xa6\x
82\x9d\xf1\xa9\x9e\x8fx\xfb\xaf|\xd92\x95\xd6\x1c\xe4\x00\xc5*\xd4\xed\xa1eg\xd7\xf4\x92\x8a#\xbe\xe9b\x08:\xf6\x94\x83gU\xb4\xd
b;\x16\xd9\xa2\xafvb\x92Z\xf8 \x07\xf8\xb0\xf9\x9b7XWF\x1d\x00\xfft\xff\xf6\x1d\xd4^o\xf2G\x0b\xac\x12\x0c\xad|\x95\xb2}\x9f\xa6
\xe1U\x9c{>`P\xe5\xb4\xf6\x81\x18\xb3\xe0\xf6E6\x96\x05a\x8e,\xda\rG_\x0fQ\xb1!\xbf\xc4\xba\x0eQ.\xe7\x8a\xc5m\xa1QR\xa5In\xdf\x
8c\xbf\xc8\xbf\xa7\xc38\x89\xf7\x85\x1a\xd3\\\xdf\x81\x08\x86Dko\x93\x9c\x0f,\x1a\x07\xafl]\xc5\xee\x88\x05\x9f\x9a\xc1\x9b\x1c\
xbf\xa2\xd5cC\x8f\x9b\x02F\xf4G\x0cY\xfe\xc6\xe0\xa4*\xfc\xf5\xab!\xaa\x15\xb3\xcb\xbe\xcd\xb1Uy\xc1\xf0m\x1c\xbb\x12\xdfk'
```

Fig 5: Encrypted message



```
Decrypted Message:
Hello, Bob! This is a secret message.
```

Fig 6: Decrypted message

DISCUSSION

The use of the proposed model in information leakage prevention demonstrated promising results, particularly on access control, data monitoring, and limits on information sharing. The simulation identified that the utilization of encryption mechanisms, multi-level authentication, and anomaly detection systems significantly reduced the risk of malicious access to information and leakage. Importantly, the multi-layer nature of the model allowed complete coverage of potential threat vectors, hence security breaches were avoided or detected easily. The system's ability to accurately determine unauthorized attempts at access made the model structure and logic valid. Having user behavior analytics and audit trail mechanisms made it important in differentiating between legitimate access and suspicious behavior. This study aligns with existing research on data leakage prevention but goes a step further to recommend a centralized and integrated model incorporating various proactive security mechanisms into one system.

Additionally, the results of the simulation also indicated that organizations could maintain system performance in implementing the model, suggesting that good security need not compromise operational efficiency. This is important for scalability and real-world adoption within business contexts. Generally, the findings indicate that the proposed model is technically possible and practically realizable. But the deployment also revealed potential limitations, such as the need for regular updates of the baselines for anomaly detection and the merit of training users to reduce vulnerabilities caused by human error.

Implications for Research and Practice

This study contributes to information security literature through the proposition of a novel model that combines existing security methods into one structure with the purpose of preventing information leakage. It offers avenues for future research, particularly the optimization of security systems combining encryption, access control, and real-time monitoring. In addition, future work can be conducted to design adaptive learning mechanisms capable of optimizing data leakage detection with respect to changing user behavior patterns. Comparative performance analysis against alternative models can also be undertaken to evaluate the proposed model's performance in terms of efficiency, scalability, and robustness in the face of different threat environments. Subsequent studies may further augment by experimenting on this model on other industries such as healthcare, banking, and public administration, in order to test its efficiency and versatility across different organizational domains. The model may also prove useful to practitioners as an operative and practical instrument for mitigating information leakage risk. It emphasizes the need for a multi-layered framework with preventive, detective, and corrective controls, backed up with continuous monitoring and audit to assist in ensuring compliance and allowing for early detection of anomalies. Importantly, the model further suggests user awareness and training as a way of optimizing the efficiency of technical controls, particularly against insider threats. Companies using this model will be able to anticipate a better information security position, reduced threat of data breach, and increased trust between clients, partners, and regulators. Its modular structure makes it adaptable to be fit into current IT systems with a minimal disruption of operations, so it is an appropriate solution for a large number of businesses.

CONCLUSION

The development of a model for preventing information leakage using the RSA public key encryption algorithm is a crucial step towards enhancing data security in various domains. RSA encryption provides a robust framework for securing sensitive information by employing a pair of keys; public and private. They play a vital role in encrypting and decrypting data. The model's effectiveness lies in its ability to ensure confidentiality and integrity of information, making it challenging for unauthorized parties to access or manipulate sensitive data.

Through the utilization of RSA encryption, organizations can establish a secure communication channel, safeguarding data during transmission and storage. The mathematical complexity underlying the RSA algorithm adds an extra layer of protection, making it resistant to attacks such as factorization of large prime numbers. This robustness contributes to the model's reliability in real-world applications where the prevention of information leakage is paramount.

However, it's essential to acknowledge that no system is entirely immune to potential threats, and continuous monitoring, updating, and adaptation of security measures are necessary to counter evolving cyber threats. Additionally, the performance considerations of RSA, particularly in resource-constrained environments, may warrant exploration of alternative cryptographic methods or hybrid approaches.

Building a model to prevent information leakage using the RSA public key encryption algorithm offers promising results. RSA's robust mathematical foundation and its ability to securely transmit data between authorized parties make it a strong candidate for data security.

In conclusion, the development of a model integrating RSA public key encryption represents a commendable stride towards bolstering information security. This model serves as a fundamental tool in the ongoing efforts to mitigate the risks associated with information leakage and unauthorized access, contributing to the overall resilience of data protection strategies in our increasingly interconnected and data-driven world.

FUTURE RESEARCH

While this research has been successful in creating and implementing a model for information leakage prevention using RSA public key encryption, there are several directions of further research that can build on and enrich this work.

Further research can be directed towards integrating adaptive machine learning models into the current encryption-based system. These models can learn anomalous behaviour patterns or policy violations dynamically by adapting to evolving user behaviour and attack vectors. This would significantly improve the system's responsiveness to zero-day attacks and unknown vulnerabilities that may not be adequately addressed by encryption.

Secondly, because RSA performance might be constrained in environments with scarce resources such as in mobile or embedded systems, an area for research in the future would be hybridizing crypto-algorithms by combining RSA with light algorithms such as ECC (Elliptic Curve Cryptography) or symmetric algorithms such as AES to find a balance between computation efficiency and security strength.

Furthermore, the success of the model would be ascertained within real-world operational contexts in various sectors such as finance, health, education, and government. Conducting case studies in these sectors will allow for the examination of the model's applicability and flexibility across various organizational architectures, regulatory requirements, and threat categories.

The other possible research field involves the use of blockchain technology to make data transaction more transparent, traceable, and accountable. By encrypting the access and movement logs for data and maintaining them on a blockchain ledger, researchers can explore the possibility of tamper-proof audit trails that improve leakage detection and forensic analysis.

In addition, future studies might involve designing a user-friendly interface for the information leakage prevention system to enhance more usability and promote higher adoption without sacrificing security. Human factors research, such as learning end-users' engagement with encryption and leakage notification, could guide interface designs that minimize operational friction and alleviate false positive fatigue.

Lastly, scholars can look at the legal, ethical, and privacy implications of automated data leakage prevention systems, particularly in scenarios where there are high compliance requirements (e.g., GDPR, HIPAA). This includes asking how encrypted data is stored, who has access to audit logs, and when user data can be decrypted for legal inspection.

REFERENCES

[1] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009) 'Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds' https://rist.tech.cornell.edu/papers/cloudsec.html.

[2] Hitaj, B., Ateniese, G., and Pérez-Cruz, F. (2017) 'Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning'. https://arxiv.org/abs/1702.07464.

[3] Yan, Z., Yu, F.R., Gong, Q., and Li, J. (2021) 'Privacy-preserving collaborative learning for mitigating indirect information leakage'. *Information Sciences*, 552, pp. 80–99. https://www.sciencedirect.com/science/article/abs/pii/S0020025520309749.

[4] Ye, T. and Li-Jiang, Z. (2022) 'Semi-quantum dialogue protocol based on four-particle Ω state'. *Optics Communications*, 518, 128278. https://www.sciencedirect.com/science/article/abs/pii/S0030401822000954.Xu, X., Zhang, [5] X., Li, W., and Liu, C. (2020) 'Blockchain-enabled accountability mechanism against information leakage in vertical industry services'. *IEEE Transactions on Network and Service Management*, 17(1), pp. 70–81. https://www.researchgate.net/publication/339542455_Blockchain-Enabled_Accountability_Mechanism_Against_Information_Leakage_in_Vertical_Industry_Services.

[6] Wong, C.W.Y., and Boon-Itt, S. (2021) 'A conceptual framework for information-leakage-resilience'. *Supply Chain Management: An International Journal*, 26(2), pp. 215–230. https://www.researchgate.net/publication/353717588_A_conceptual_framework_for_information-leakage-resilience.

[7] Song, C. and Raghunathan, A. (2020) 'Information Leakage in Embedding Models'. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*, pp. 377–390. https://arxiv.org/abs/2004.00053.

[8] Giechaskiel, I. and Eguro, K., 2016. *Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires*. arXiv preprint arXiv:1611.08882. https://arxiv.org/abs/1611.08882.

[9] Zajić, A. and Prvulović, M., 2014. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Transactions on Electromagnetic Compatibility*, 56(4), pp.885–893. https://bpb-us-e1.wpmucdn.com/sites.gatech.edu/dist/4/463/files/2015/06/TEMC_314_2013.pdf.

[10] Zhang, J. and Situ, H., 2016. *Information Leakage in Efficient Bidirectional Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom*. arXiv preprint arXiv:1606.07188. https://arxiv.org/abs/1606.07188

[11] Liu, W., Liu, C. and Wang, Y., 2016. Information leakage problem in high-capacity quantum secure communication with authentication using Einstein-Podolsky-Rosen pairs. *Chinese Physics Letters*, 33(7), p.070305. https://cpl.iphy.ac.cn/article/10.1088/0256-307X/33/7/070305

[12] Ritzdorf, H., et al., 2016. On information leakage in deduplicated storage systems. *Proceedings of the 8th ACM SIGSAC Symposium on Cloud Computing*, pp.187–200. https://dl.acm.org/doi/10.1145/2976749.2978311

[13] Hannun, A., Guo, C. and van der Maaten, L., 2021. *Measuring Data Leakage in Machine-Learning Models with Fisher Information*. arXiv preprint arXiv:2102.11673. https://arxiv.org/abs/2102.11673

[14] Hauer, B., 2015. Data and information leakage prevention within the scope of information security. *International Journal of Computer and Communication Engineering*, 4(4), pp.254–259. https://www.researchgate.net/publication/286381958_Data_and_Information_Leakage_Prevention_Within_the_Scope_of_Information_Security

[15] Polisetty, S.K. and Mutyalu, K.V., 2012. Development of data leakage detection using data allocation strategies. *International Journal of Computer Trends and Technology (IJCTT)*, 3(4), pp.438–442.

[16] Alneyadi, S., Sithirasenan, E. and Muthukkumarasamy, V. (2021) 'A survey on data leakage prevention systems', *Journal of Network and Computer Applications*, vol. 62, pp. 137–152. doi:10.1016/j.jnca.2020.01.008.

[17] Papadimitriou, P. and Molina, H.G. (2022) 'Data Leakage Detection', *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 1, pp. 51–63.

[18] Huang, X., Lu, Y., Li, D., and Ma, M., (2018)**.** A novel mechanism for fast detection of transformed data leakage. *IEEE Access*, https://www.researchgate.net/publication/326054308_A_Novel_Mechanism_for_Fast_Detection_of_Transformed_Data_Leakage.

[19] Al-Anie, H.K., Alia, M.A. and Hnaif, A.A. (2011) 'eVoting Protocol Based on Public-Key Cryptography', *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, no. 4, pp. 87–98.

[20] Cheng, L., Liu, F. and Yao, D. (2022) 'Enterprise data breach: causes, challenges, prevention, and future directions', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 5, e1211.

[21] Katz, G., Elovici, Y. and Shapira, B. (2020) 'Coban: A context-based model for data leakage prevention', *Information Sciences*, vol. 262, pp. 137–158. doi:10.1016/j.ins.2020.10.005.