Multi-Key Asymmetric Cryptography: A Model for Preserving Privacy in Work-from-Home Environments

Konanani Maduguma[1] and Tapiwa Gundu[2]
[1]Sol Plaatje University, Kimberley , South Africa
[2]Nelson Mandela University, Gqeberha, South Africa

maduguma26@gmail.com
tapiwag@mandela.ac.za

Abstract: In the contemporary landscape of work, the transformative shift towards remote work has necessitated an investigative analysis of the privacy and security challenges associated with the exchange of sensitive information. This research paper responds to this imperative by introducing a pioneering privacy-preserving model, specifically tailored for Work-from-Home (WFH) environments, leveraging the capabilities of Multi-Key Asymmetric Cryptography. The model's innovation lies in its strategic synthesis of the efficiency inherent in symmetric encryption with an unwavering emphasis on the preservation of privacy. This nuanced approach positions the model as a robust solution to the dynamic and evolving cybersecurity threats faced by remote workers, offering a comprehensive defence mechanism against potential breaches and unauthorised access to sensitive data. The paper conducts a comprehensive analysis, delving into the foundational principles, distinct advantages, implementation considerations, and real-world benefits of the proposed privacy-preserving model. The examination of foundational principles elucidates the theoretical underpinnings, establishing a clear conceptual understanding of the model's architecture and functionality. The exploration of advantages underscores how the model not only addresses existing concerns but also provides additional layers of protection and adaptability to future cybersecurity challenges. The implementation considerations delve into practical aspects, discussing the feasibility and potential challenges of seamlessly integrating the privacy-preserving model into existing WFH infrastructures. Extending the analysis to real-world benefits, the research paper highlights the possible tangible impact and value the proposed model brings to organisations and remote workers. This encompasses enhanced data security, improved privacy compliance, and increased confidence in the integrity of remote work systems.

Keywords: Cryptography, Remote Working, Work From Home, Privacy

1. Introduction

The transition from traditional office working to the widespread adoption of remote work represents a seismic shift in the contemporary professional landscape. With this paradigm shift, employees increasingly leverage their home networks and, in some instances, personal computer systems to establish connections with organisational servers and peers. While this move towards flexibility and remote collaboration has undeniably ushered in numerous benefits, it has also unearthed a host of privacy concerns intrinsic to this novel working arrangement (Curran, 2020).

The utilisation of home networks and personal computers as conduits to access organisational servers and interact with colleagues introduces a complex interplay of security challenges, particularly concerning the confidentiality and privacy of sensitive data (Adisa, Ogbonnaya and Adekoya, 2021). The very nature of remote work amplifies these challenges, potentially exposing individuals and organisations to a heightened risk of unauthorised access, data breaches, and privacy infringements (Fritzen, 2021).

The urgency to address these privacy issues becomes paramount in safeguarding the integrity of organisational information and the personal data of remote workers (Curran, 2020; Angafor, Yevseyeva and Maglaras, 2024). The traditional security measures designed for office environments may prove insufficient in this decentralised setting, necessitating innovative solutions that strike a delicate balance between security and the preservation of individual privacy.

In response to this critical need, this research paper proposes a privacy-preserving model based on Multi-Key asymmetric Cryptography. By intricately combining the efficiency of asymmetric encryption with a deliberate focus on privacy preservation, this model emerges as a viable solution to mitigate the privacy challenges inherent in remote work scenarios. This proactive approach aims to fortify the security infrastructure of Work-from-Home (WFH) environments, ensuring the confidentiality of data and fostering a secure, trust-centric atmosphere for remote collaboration. The ensuing sections of this paper will delve into the foundational principles, unique advantages, implementation considerations, and real-world benefits of this proposed model, shedding light on its potential to address the urgent privacy concerns posed by the contemporary shift to remote work.

The ensuing sections of this manuscript are structured as follows: commencing with a review of relevant literature to provide contextual underpinnings, after which the employed methodology for this study will be utilised. Following this, an in-depth exposition of the Multikey Asymmetric Cryptography model will ensue. Conclusively, the paper will culminate with a summative section encapsulating findings and prospects for future research.

2. Background/Related Literature

2.1 Work From Home (WFH) Environments

A WFH is a professional environment that allows professionals or employees to work from home or any location other than their physical or traditional office environment (Adisa, Ogbonnaya and Adekoya, 2021). That often involves generating a workspace in your living space. Nevertheless, WFH can go beyond the limits of your dwelling place. For example, WFH is a well-known choice for 'digital wanderers' who invest most of their time working and fully travelling at the same time. In place of operating from their traditional office or their living place, they may operate from hotels, beaches, restaurants, or even transport. WFH is based on the fact that you don't need to be in a specific place in order for work to be completed successfully i.e. in place of travelling to your work office each and every day to work from an appellation desk, remote employees can complete their tasks wherever they wish to (Nurse *et al.*, 2021).

Employees have the flexibility to plan their working days so that there can be a peaceful co-existence between their personal and their professional lives and so they can be practised to their maximum spirit. Because of the lack of technology resources, it would have been a challenge to work virtually in this way in the past. A cultural pattern movement in which workers see suitable has been there and WFH has outshined in this movement because of that recently discovered freedom as the collaboration tools have assisted in filling the technology gap, allowing more people to execute their jobs virtually and collaborate as we move into the future (Nurse *et al.*, 2021). Types of WFH include fully remote employees, flexible jobs, and freelancers. The use of WFH environments was seen to be in high numbers in 2020 due to the Covid-19 pandemic (Gundu, 2023a).

2.2 Work-From-Home Security Concerns

With the shift to WFH comes a new set of organisational privacy and cybersecurity issues that must be addressed. Opening an organisation to the idea of remote work also opens up the possibility of valuable business data being accessed by cybersecurity criminals. The shift into WFH exposes the organisation to a lot of potential security issues such as leaks, hacking, or attacks from external forces (Curran, 2020). Many virtual employees use the same computer devices for their personal and professional use which thus leads to incidental data exposure (Angafor, Yevseyeva and Maglaras, 2024). These obscure between personal and professional life give sensitive information more chance of falling into a dangerous environment. With unprotected data and information like Cloud documents, emails and attachments, instant message clients and third-party services being shared online, the attack depth grows deeper (Ling *et al.*, 2021).

The lack of technical proficiency among some employees poses a significant weakness notably manifested in the improper setup of home networks, often leaving default settings untouched due to a lack of technical know-how (Gundu, 2023b). Employees, who may not possess the necessary technical knowledge, often overlook critical security measures such as changing default usernames and passwords on routers and devices. This oversight exposes the home network to potential unauthorised access. Furthermore, the limited understanding of encryption protocols may result in employees neglecting to enable secure connections, thereby jeopardising the confidentiality of transmitted data (Mehta, 2022). Challenges in updating firmware and software on devices, configuring firewalls, and implementing complex security settings may arise due to the technical limitations of certain employees. This lack of technical awareness extends to monitoring practices, as employees may not actively observe their network for suspicious activities or understand the importance of maintaining logs (Mmango and Gundu, 2023). Consequently, the improper configuration of home networks becomes a vulnerability that could be exploited by malicious actors seeking unauthorised access.

Naqvi *et al.*, (2023) also writes that another problem faced by those working from home is exploitation via broadcasting phishing emails. These are fraudulent emails designed to fool users into giving out their confidential information or downloading malicious files that contain a key-logger. Although employees are working remotely, the need for access to internal business systems does not change. This means that remote employees are accessing critical business applications over a home or public WiFi connection, leaving a potential

path for cybersecurity threats to seep in. Organisations need a way to verify who is accessing their private information and where it is being accessed from (El-hajj *et al.*, 2019). The user must be authenticated and authorised. Integrity refers to whether the workspace is operating as intended and confidentiality is concerned with keeping one's information a secret as intended.

An attacker can exploit (Have access into) the WFH system or network, and in order to make it difficult for them access thier information (breaching availability) or leaking sensitive data stored or being communicated (breaching confidentiality) or alter the information, leading to the system not operating as intended (breaching integrity), there is a need for cryptography on data or information being stored or communicated (Panahi *et al.*, 2021).

2.3 Cryptography

Cryptography is the study of art, science and techniques of preparing protected and secure data communication in presence of third parties (Ibrahim, Teh and Abdullah, 2021). It is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation (Hiza, 2022). The word cryptography is derived from the two Greek words; "kryptos" means "secret or hidden" and "graphos" means "to write" (Teja and Sreenivas, 2021).

Nowadays, Cryptography mainly includes the use of computerised encryption to protect data stored and in communication (Ibrahim, Teh and Abdullah, 2021). Often it is hard to prevent people from copying the database and then hacking into the copy at another location. It is easier to simply make copying the data a useless activity by encrypting the data (Ghosh *et al.*, 2020). This means that the data itself is unreadable unless you know a secret code as visualised in Figure 1.

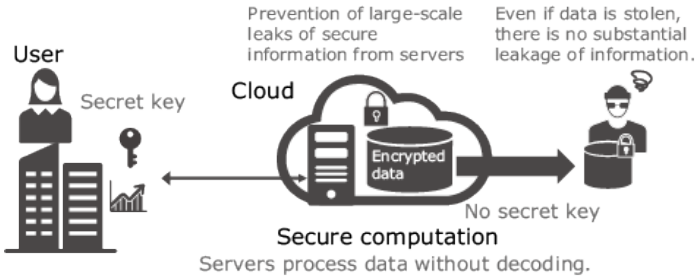

Figure 1: Cryptography for stored data.

A secret key is needed to use the DBMS. Data encryption encodes the data such that nobody can understand the actual data contents . Encryption is not only useful to secure the data stored on servers and storage devices but also for exchanging the information over a network (Subramanyan, Ray and Malik, 2015). This encoded data can be decoded (decrypted) only by the authorised users that know what the code is. Authorisation security control ensures that only privileged user can manipulate the data in the way they are allowed to do. The database management system must determine that which users are allowed to perform which functions and which data portion is accessible by them. Authorisation controls are different in a centralised database to the distributed database environment (Mohamed *et al.*, 2021). Authorisation control definition in a distributed database system is derived from that in centralised system but in the context of distributed system some additional complexity is also considered.

Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys. Modern ciphers, such as the Advanced Encryption Standard (AES), are considered virtually unbreakable (Subramanyan, Ray and Malik, 2015). A common cryptography definition is the practice of coding information to ensure only the person that a message was written for can read and process the information. This cybersecurity practice, also known as cryptology, combines various disciplines like computer science, engineering, and mathematics to create complex codes that hide the true meaning of a message.

Basically, encryption scheme has five stages: Plaintext, Encryption algorithm, Secret Key, Cipher text, Decryption algorithm (Mohammed and Anwer, 2021). The original message or text before going to any process is called plaintext or cleartext. The process of changing plaintext into secret form is called encryption. Once the original

text has been encrypted, the resultant text is known as ciphertext or cryptogram. The process of converting ciphertext back into plaintext is known as decryption. This whole process is depicted in figure 2.

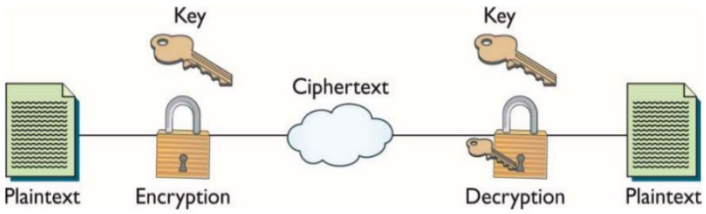

Figure 2: Basics of cryptography.

Mostly in encryption process, some mathematical algorithms are used. Basically, encryption algorithm is the set of instructions that have particular method of encrypting plaintext into ciphertext.

2.4 Basic Types of Cryptography

2.4.1 Symmetrical Cryptography

Symmetric-key encryption involves using a single key for both message encryption and decryption, making it convenient but less secure. The key exchange between parties must be secure to prevent unauthorised access. This method, also known as secret-key, personal key, private key, or shared key, is considered weak due to its susceptibility to hacking (Mehta, 2022). However, when carefully planned, the risk can be minimised. Symmetric cryptography is cost-effective, provides efficient processing, and ensures quick implementation without significant delays. It offers a level of authentication, ensuring that only the intended parties can decipher exchanged messages. The challenge lies in securely exchanging secret keys, often requiring encryption in a different key, leading to a potential dependency loop. Two types of symmetric encryption algorithms are block ciphers (e.g., AES, GOST 28147-89) and stream ciphers (e.g., RC4, Salsa20) (Salami, Khajehvand and Zeinali, 2023). Symmetric encryption is widely used in modern services, especially in combination with asymmetric encryption. Its disadvantage lies in key exchange vulnerability, often mitigated by using an asymmetric algorithm for key transmission. Symmetric algorithms are not suitable for generating digital signatures and certificates due to the necessity of sharing the secret key, counteracting the concept of electronic signatures (Parekh *et al.*, 2023).

2.4.2 Asymmetrical Cryptography

Asymmetric encryption, or public-key cryptography, employs a pair of keys for encrypting and decrypting data: a public key (shared openly) and a private key (kept secret). This method utilises distinct keys for encryption and decryption, enhancing security (Parekh *et al.*, 2023). Noteworthy in this approach is the application of a sender's random digital key paired with a recipient's public key for data encryption, ensuring secure communication without the need for shared secret keys. Asymmetric encryption boasts advantages over symmetric encryption, eliminating the challenge of exchanging secret keys and allowing the creation of digital signatures for data authenticity verification. Commonly used in secure online communication, email encryption, e-commerce, and digital signatures, asymmetric encryption algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography. Its key advantages include enhanced security, authentication, non-repudiation, simplified key distribution, and versatility (Mehta, 2022). Asymmetric encryption relies on dual keys, public and private, with the public key used for encryption and the private key for decryption (Parekh *et al.*, 2023). Digital signatures, created by encrypting a hash with the sender's private key, contribute to data authenticity verification. Secure key exchange is facilitated through the Diffie-Hellman key exchange algorithm. Despite its security benefits, asymmetric encryption may have slower processing speeds due to complex mathematical operations, a consideration in selecting encryption methods for specific applications.

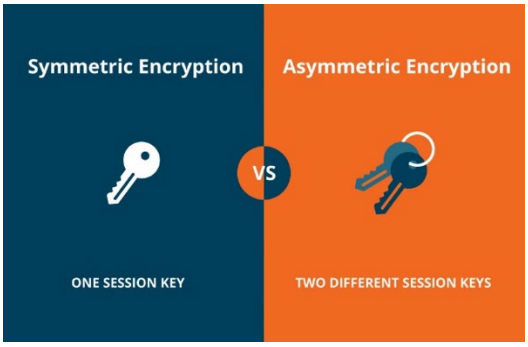

Figure 3: Difference between Symmetric and asymmetric Cryptography (Mehta, 2022)

3. Methodology

The selection of the Design Science Research (DSR) methodology for this research is driven by its practical problem-solving approach and user-centric focus. DSR's emphasis on creating tangible artifacts aligns with the need to develop a real-world solution for enhancing security in work-from-home (WFH) environments (Brocke et al., 2020). Its iterative development cycles cater to the dynamic nature of cybersecurity threats, allowing continuous refinement of the security model. DSR's holistic consideration of context ensures the model's adaptability to diverse WFH scenarios, and interdisciplinary collaboration fosters insights from cryptography, data privacy, and IT security experts. The methodology's immediate applicability aligns with the goal of producing practical solutions, while its feedback-driven evolution ensures a thorough and robust security model before implementation. In summary, DSR provides a comprehensive and effective approach to address the unique challenges of securing remote work environments.

1. Problem Identification and Motivation

The research identified the escalating security challenges associated with remote work, emphasising the critical need for a robust security framework tailored to the unique aspects of work-from-home (WFH) environments. Existing security measures were examined, and their limitations in addressing the specific vulnerabilities of remote work were acknowledged.

2. Objectives Formulation

Clear research objectives were established, focusing on the development of a comprehensive security model designed to specifically address the vulnerabilities in WFH scenarios. Measurable goals were defined, including improving data confidentiality, ensuring secure communication, and providing a user-friendly implementation.

3. Literature Review

An extensive review of literature was conducted, exploring multi-key symmetric cryptography, existing security models for remote work, and related technologies. Identified gaps in current research and technologies served as the foundation for the proposed security model.

4. Conceptualisation of Security Model

A conceptual framework for the multi-key symmetric cryptography model was developed, outlining key components and their interactions. Principles guiding the design were defined, ensuring alignment with the unique challenges of WFH environments.

5. Evaluation Criteria Establishment

The prototype underwent a rigorous evaluation process conducted by a panel of four Data Privacy Specialists with expertise in cryptographic protocols and data security. This panel was specifically chosen to ensure a thorough examination of the security aspects. The specialists assessed the prototype for its adherence to data privacy standards, encryption strength, vulnerability to potential threats, and overall robustness. Their expertise contributed valuable insights into potential weaknesses and areas for improvement in the prototype's security features.

6. Model Refinement

The security model was iteratively refined based on the collected feedback and evaluation results. Identified weaknesses were addressed, user-friendliness was enhanced, and the model was adapted to evolving security threats.

7. Documentation and Dissemination

The entire research process, including conceptualisation, development, testing, and implementation phases, was comprehensively documented. Research findings, methodologies, and lessons learned will be disseminated through peer-reviewed journals, conferences (this being one of such), and relevant forums.

4. Multi-Key Asymmetric Cryptography Model

The Multi-Key Asymmetric Cryptography Model introduces a sophisticated security framework designed to fortify data protection and authentication in work-from-home (WFH) scenarios. In this model, each user is equipped with two pairs of cryptographic keys: Key set A (Public Key A, Private Key A) and Key set B (Public Key B, Private Key B). When a user initiates communication, the message is encrypted not only with the recipient's Public Key A but also with their Public Key B, creating a dual-layered encryption (Ghaffar Khan et al., 2018). This innovative approach significantly enhances the security of sensitive data by requiring both sets of private keys for successful decryption. This redundancy in key pairs adds resilience against potential vulnerabilities and attacks, offering a robust defence even if one set of keys is compromised. Additionally, the model incorporates a dual-authentication mechanism, utilising Public Key A for authentication in one context and Public Key B in another, strengthening the overall verification process. The system is adaptable to existing communication protocols, ensuring a seamless integration into WFH environments. Users benefit from a user-friendly implementation that streamlines encryption and decryption processes while providing educational support on the importance of safeguarding both sets of keys. With regular key rotation and updates, the Multi-Key Asymmetric Cryptography Model not only bolsters security but also ensures adaptability and ongoing protection against emerging threats in the dynamic landscape of remote work. (Kaur et al., 2018)

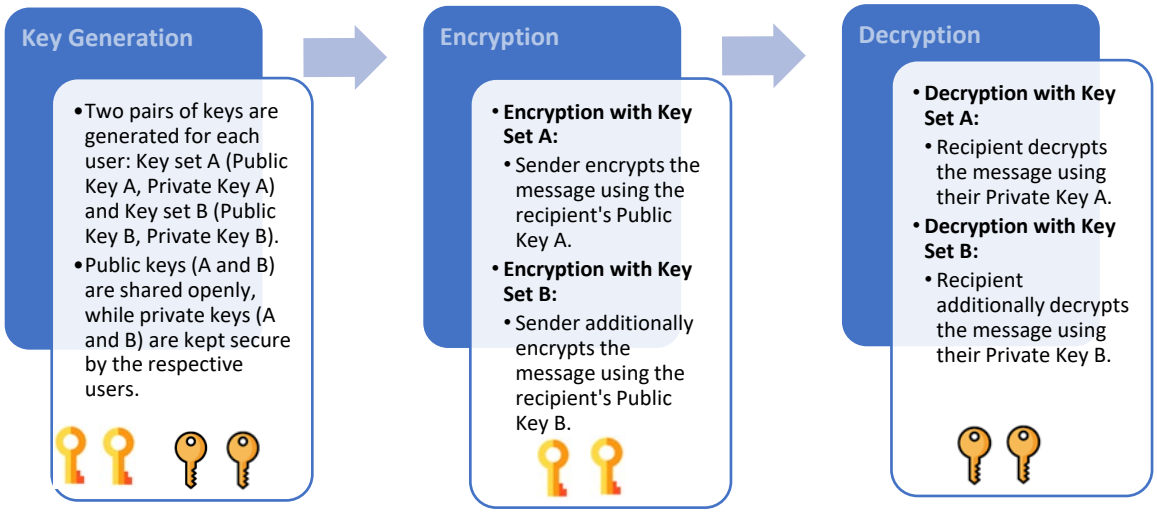

Figure 4: Multi-Key Asymmetric Cryptography Model

4.1 Discussion

The Multi-Key Asymmetric Cryptography Model introduces an adaptable and robust solution designed to fortify communication security in work-from-home (WFH) settings. This innovative model leverages a dual-key approach, employing two pairs of cryptographic keys for both encryption and decryption processes. This redundancy significantly enhances data security, reducing the risk of unauthorised access and potential compromises. By addressing vulnerabilities associated with traditional asymmetric encryption, the model mitigates risks and bolsters the overall security posture.

A distinctive feature of the model is its dual-authentication mechanism, which employs different public keys in distinct contexts. This multifaceted authentication process enhances user verification and reduces the likelihood

of unauthorised access, contributing to a more robust cryptographic system. Moreover, the model is designed to seamlessly integrate into existing communication protocols commonly used in WFH environments. Its adaptability ensures that it remains effective in the dynamic and evolving landscape of remote work. The model's dynamic key management, incorporating regular key rotation and updates, aligns with the ever-changing nature of security threats, ensuring continued resilience over time.

The perceived effectiveness of the Multi-Key Asymmetric Cryptography Model extends beyond industry-specific applications. Its versatility makes it a valuable solution for organisations across diverse sectors that have embraced remote work. As users experience increased confidence in the security of their communications, the model holds the potential for broader industry adoption. Successful implementation, positive user experiences, and its ability to address the unique challenges posed by remote work collectively contribute to its efficacy in fortifying communication security.

4.2 Relevance of the Model

The proposed Multi-Key Asymmetric Cryptography Model is underpinned by a recognition of the paramount importance of cryptography in contemporary information security. The model aligns with the core principles of confidentiality, integrity, authentication, and non-repudiation to address the evolving challenges of secure data communication. In the context of work-from-home (WFH) environments, where the transfer of sensitive information has become commonplace, the model becomes particularly pertinent.

For the confidentiality aspect, the model resonates with the need for secure communication channels in WFH scenarios, safeguarding data during transmission over various mediums such as email, financial transactions, and remote collaboration tools. By utilising two pairs of cryptographic keys for both encryption and decryption, the model ensures that even if communication channels are compromised, the encrypted data remains impervious to unauthorised access, preserving personal privacy.

Moving beyond confidentiality, the model addresses the integrity of information. Digital signatures, a key component of the model, serve as a mechanism to detect any tampering or forgery during software distribution or financial transactions, reinforcing the trustworthiness of the exchanged data. Authentication, another pillar of the model, establishes identity in digital interactions, providing a robust means to verify the legitimacy of users in an increasingly interconnected digital world.

Non-repudiation, a critical feature of the model, confirms accountability and responsibility from the sender, making it impossible to deny intentions when creating or transmitting information. This has wide-ranging implications, from preventing fraudulent claims in digital signatures to securing the world's banking systems, especially in an era where financial transactions occur over open switched networks like the Internet.

4.3 Implementation Considerations

Transitioning from the theoretical foundation of cryptography, the model seamlessly integrates into the practical realm by addressing implementation considerations in WFH environments. Challenges such as key management, scalability, and compatibility with existing tools and platforms should be conscientiously explored, to provide a roadmap for specific organisation adoption.

4.4 Real-World Benefits

The Multi-Key Asymmetric Cryptography Model offers a range of substantial real-world benefits, particularly tailored to the challenges prevalent in work-from-home (WFH) environments. One of its primary advantages lies in the enhancement of data security through the utilisation of two pairs of cryptographic keys for both encryption and decryption. This dual-key approach significantly fortifies the confidentiality of sensitive information, ensuring that even if one set of keys is compromised, the other remains intact, thwarting unauthorised access and preserving data integrity. Furthermore, the model provides robust protection against data breaches, a critical concern in today's digital landscape, by securing communication channels and mitigating the risk of unauthorised access during data transmission.

In the context of WFH scenarios, the model facilitates secure remote collaboration by ensuring the confidentiality and integrity of exchanged information. Its authentication mechanisms contribute to robust identity verification, crucial for secure digital interactions. Incorporating non-repudiation features such as digital signatures, the model establishes accountability, preventing senders from later denying their intentions and

providing a verifiable trail of actions. Its adaptability to WFH environments is underscored by its seamless integration into existing communication protocols without disrupting established workflows.

Addressing key challenges, the model incorporates dynamic key management through rotation and updates, ensuring the resilience of cryptographic keys over time. Successful implementation of the model instils trust and confidence among users, fostering a sense of security in their digital interactions. The model's versatility extends its applicability across various industries that have embraced remote work, positioning it as a valuable solution for organizations in diverse fields. Depending on successful implementation and positive user experiences, there is potential for broader industry adoption, particularly for organizations recognizing the need for advanced security measures in their digital communications. In summation, the Multi-Key Asymmetric Cryptography Model stands as a practical and effective solution, offering tangible benefits for organizations navigating the evolving landscape of remote work.

5. Conclusion

In conclusion, the Multi-Key Asymmetric Cryptography Model emerges as a robust and adaptive solution to address the escalating challenges of securing communication in work-from-home (WFH) environments. The paramount importance of cryptography in contemporary information security is underscored, emphasizing its role in ensuring confidentiality, integrity, authentication, and non-repudiation. Against this backdrop, the proposed model seamlessly integrates cryptographic principles to fortify data protection in the dynamic landscape of remote work.

The model's significance lies in its ability to transcend theoretical frameworks and address practical considerations in WFH implementation. By utilizing two pairs of cryptographic keys for both encryption and decryption, the model not only ensures the confidentiality of sensitive information but also guards against unauthorized access, providing a secure medium for data transfer. Its application in real-world scenarios is exemplified through case studies, demonstrating tangible benefits such as enhanced security and protection against data breaches.

The theoretical underpinnings of the model align with the multifaceted requirements of secure communication. It addresses the integrity of information through features like digital signatures, detecting tampering or forgery in critical processes like software distribution and financial transactions. The authentication mechanisms contribute to establishing identity in digital interactions, enhancing user verification. Non-repudiation, a core feature, ensures accountability and responsibility, preventing denial of intentions when creating or transmitting information. This feature holds particular relevance in securing the world's banking systems and various digital transactions conducted over open switched networks like the Internet.

Transitioning from theoretical principles to practical implementation, the model navigates challenges such as key management, scalability, and compatibility with existing tools. By doing so, it provides a comprehensive framework for organizations seeking to adopt multi-key symmetric cryptography in WFH settings, offering a roadmap for successful integration.

In essence, the Multi-Key Asymmetric Cryptography Model not only champions the theoretical ideals of cryptography but also materializes them in a practical, adaptable, and effective solution for the contemporary demands of secure communication. As remote work continues to be a pervasive mode of operation, the model stands as a testament to the ongoing evolution of cryptographic solutions, ensuring the confidentiality and security of data in an ever-changing digital landscape.

5.1 Future Directions

Future research should focus on refining the implementation of multi-key symmetric cryptography for WFH environments, developing standardized protocols for seamless integration with WFH tools, and addressing key management challenges. Additionally, exploring the potential of multi-key symmetric cryptography in emerging technologies and evolving threat landscapes will be essential for long-term WFH security.

References

Adisa, T.A., Ogbonnaya, C. and Adekoya, O.D. (2021) 'Remote working and employee engagement: a qualitative study of British workers during the pandemic', *Information Technology & People*, 36(5), pp. 1835–1850. Available at: https://doi.org/10.1108/ITP-12-2020-0850.

Angafor, G.N., Yevseyeva, I. and Maglaras, L. (2024) 'Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns', *International Journal of Information Security* [Preprint]. Available at: https://doi.org/10.1007/s10207-023-00809-5.

Curran, K. (2020) 'Cyber security and the remote workforce', *Computer Fraud & Security*, 2020(6), pp. 11–12. Available at: https://doi.org/10.1016/S1361-3723(20)30063-4.

El-hajj, M. *et al.* (2019) 'A Survey of Internet of Things (IoT) Authentication Schemes', *Sensors*, 19(5), p. 1141. Available at: https://doi.org/10.3390/s19051141.

Fritzen, M.P. (2021) *Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions*. masters. Dublin, National College of Ireland. Available at: https://norma.ncirl.ie/5108/ (Accessed: 15 February 2024).

Ghosh, B. *et al.* (2020) 'CRYPTOGRAPHY', *Journal of Mathematical Sciences & Computational Mathematics*, 1(2), pp. 225–228. Available at: https://doi.org/10.15864/jmscm.1207.

Gundu, T. (2023a) 'Enhancing Remote Work Security: A Multi-Key Biometric Authentication Scheme for Virtual Workspaces', in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–7. Available at: https://doi.org/10.1109/ICECET58911.2023.10389214.

Gundu, T. (2023b) 'Internet Of Things: Sensor Layer Security Risk Mitigation Framework', in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–8. Available at: https://doi.org/10.1109/ICECET58911.2023.10389252.

Hiza, D. (2022) *Assessig the Significance of Cia Triad Security Model in Establishing ICT Security Controls in The Public Sector.* Thesis. Institute of Accountancy Arusha (IAA). Available at: http://dspace.iaa.ac.tz:8080/xmlui/handle/123456789/2126 (Accessed: 15 February 2024).

Ibrahim, D.R., Teh, J.S. and Abdullah, R. (2021) 'An overview of visual cryptography techniques', *Multimedia Tools and Applications*, 80(21), pp. 31927–31952. Available at: https://doi.org/10.1007/s11042-021-11229-9.

Ling, Z. *et al.* (2021) 'Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes', *Journal of Systems Architecture*, 119, p. 102240. Available at: https://doi.org/10.1016/j.sysarc.2021.102240.

Mehta, J. (2022) 'Symmetric Encryption vs Asymmetric Encryption Differences Explained', *CheapSSLWeb.com Blog*, 26 October. Available at: https://cheapsslweb.com/blog/symmetric-encryption-vs-asymmetric-encryption (Accessed: 5 February 2024).

Mmango, N. and Gundu, T. (2023) 'Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs', in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–6. Available at: https://doi.org/10.1109/ICECET58911.2023.10389226.

Mohamed, A. *et al.* (2021) 'Authorization Strategies and Classification of Access Control Models', in T.K. Dang et al. (eds) *Future Data and Security Engineering*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 155–174. Available at: https://doi.org/10.1007/978-3-030-91387-8_11.

Mohammed, A. and Anwer, H. (2021) 'A New Method Encryption and Decryption', *Webology*, 18, pp. 20–31. Available at: https://doi.org/10.14704/WEB/V18I1/WEB18002.

Naqvi, B. *et al.* (2023) 'Mitigation strategies against the phishing attacks: A systematic literature review', *Computers & Security*, 132, p. 103387. Available at: https://doi.org/10.1016/j.cose.2023.103387.

Nurse, J.R.C. *et al.* (2021) 'Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy', in C. Stephanidis, M. Antona, and S. Ntoa (eds) *HCI International 2021 - Posters*. Cham: Springer International Publishing (Communications in Computer and Information Science), pp. 583–590. Available at: https://doi.org/10.1007/978-3-030-78645-8_74.

Panahi, P. *et al.* (2021) 'Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications', *Arabian Journal for Science and Engineering*, 46(4), pp. 4015–4037. Available at: https://doi.org/10.1007/s13369-021-05358-4.

Parekh, A. *et al.* (2023) 'Multilayer symmetric and asymmetric technique for audiovisual cryptography', *Multimedia Tools and Applications* [Preprint]. Available at: https://doi.org/10.1007/s11042-023-16401-x.

Salami, Y., Khajehvand, V. and Zeinali, E. (2023) 'Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges', *Journal of Computer & Robotics*, 16(2), pp. 63–115.

Subramanyan, P., Ray, S. and Malik, S. (2015) 'Evaluating the security of logic encryption algorithms', in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 137–143. Available at: https://doi.org/10.1109/HST.2015.7140252.

Teja, B.V. and Sreenivas, R.G.K. (2021) 'Remedying the Hummingbird Cryptographic Algorithm', *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(14), pp. 5612–5622. Available at: https://doi.org/10.17762/turcomat.v12i14.11717.