


Dual User Profiles: A Secure and Streamlined MDM Solution for the Modern Corporate Workforce

Ighovwerha Doghudje and Oluwafemi Akande

Abstract

The ever-increasing integration of mobile devices in the workplace necessitates robust Mobile Device Management (MDM) solutions to guarantee data security and user convenience. This study proposes a novel approach, leveraging dual user profiles on modern smartphones, to enhance security, productivity, and user experience in BYOD environments. We explored the challenges and risks associated with BYOD, emphasizing the need to balance convenience with robust data protection. We examine how MDM secures various mobile endpoints and highlight its data security, device management, and compliance functionalities. Our proposed dual-user-based MDM solution utilizes distinct personal and work profiles to isolate data, minimizing security risks and unauthorized access. We discuss its strengths, challenges, and hardware/software considerations, emphasizing the need for seamless integration, user adoption, and ongoing education. Furthermore, we present a comprehensive life cycle methodology for implementing the proposed MDM solution, incorporating security considerations throughout the deployment process. This methodology encompasses five phases: initiation, development, implementation, operations and maintenance, and disposal. The benefits of the proposed MDM include enhanced data security through features like preventing unauthorized access, remote wipe, encryption, and access controls.

Excellence in Peer-Reviewed
Publishing:


Creative Commons License Notice:

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0).

You are free to:

Share: Copy and redistribute the material in any medium or format.

Adapt: Remix, transform, and build upon the material for any purpose, even commercially.

Under the following conditions:

Attribution: You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike: If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. Please visit the Creative Commons website at <https://creativecommons.org/licenses/by-sa/4.0/>.



INTRODUCITON

The increasing integration of mobile devices into the fabric of modern organizations has necessitated the establishment of robust Mobile Device Management (MDM) systems (Sisala & Othman, 2020). As the reliance on mobile devices grows, so does the need for sophisticated approaches to secure and manage these devices effectively (Wang et al., 2014b). In this context, our study explores a novel approach, Dual User Profiles for MDM. This promising paradigm brings together hardware and software considerations to enhance the security and functionality of mobile devices in enterprise settings. Mobile Device Management (MDM) stands as a linchpin in the overarching framework of Enterprise Mobility Management (EMM), empowering organizations to orchestrate the deployment, configuration, and security of mobile devices (Jalili, 2014). The increasing prevalence of personal mobile devices in the



workplace, often called Bring Your Device (BYOD), poses unique challenges that organizations must navigate to balance convenience and security.

In this study, we scrutinize the foundational components of MDM, exploring its multifaceted role in securing, monitoring, and managing mobile devices across the enterprise. Addressing the challenges posed by BYOD, privacy concerns, and the evolving landscape of mobile endpoints, we uncover the complexities inherent in ensuring data security while optimizing user experience. To bolster the efficacy of MDM in securing endpoints, we propose a Dual User-Based MDM Solution. Leveraging the dual user features inherent in modern smartphones; our approach envisions distinct user profiles for personal and work-related activities. This segregation enhances security by isolating personal and work data, mitigating the risks of data breaches and unauthorized access. The proposed solution has strengths and challenges, considering hardware and software aspects. We emphasize the need for seamless integration with existing MDM solutions, user adoption, and ongoing education (Singh, 2023). Additionally, we provide a comprehensive life cycle methodology for implementing MDM solutions, addressing initiation, development, implementation, operations and maintenance, and disposal phases.

UNDERSTANDING MDM

Mobile Device Management (MDM) is a critical component of Enterprise Mobility Management (EMM) that enables organizations to secure, monitor, manage, and support mobile devices deployed across the enterprise (Yamin & Katt, 2019), (Batool & Masood, 2020). MDM software provides a centralized platform for IT administrators to manage the entire lifecycle of mobile devices, including device configuration, application management, data security, and user authentication. The primary goal of MDM is to optimize the functionality and security of a mobile communication network while minimizing cost and downtime. This applies to both company-owned and employee-owned devices across the enterprise.

a Mobile Device Management (MDM)

This component allows IT administrators to manage and secure mobile devices, including smartphones, tablets, and laptops. MDM software enables IT to configure devices remotely, apply security policies, and monitor device status.

b Mobile Application Management (MAM)

This component allows IT administrators to manage and secure mobile applications. MAM software enables IT to distribute, update, and remove applications from mobile devices.

c Mobile Content Management (MCM)

This component allows IT administrators to manage and secure mobile content, including documents, files, and email. MCM software enables IT to distribute, update, and remove content from mobile devices.

d Mobile Security Management (MSM)

This component allows IT administrators to manage and secure mobile devices against security threats. MSM software enables IT to implement security policies, encrypt data, and monitor device status.

CHALLENGES AND RISKS

This section comprehensively explores challenges and risks associated with personal mobile devices, privacy concerns, and the ongoing quest to balance convenience with security in the ever-evolving landscape of mobile endpoints.

Personal Mobile Devices (BYOD) in the Workplace

Addressing the challenges posed by personal mobile devices in the workplace, commonly known as Bring Your Device (BYOD), is a critical consideration (“Solutions to a Balanced Approach between Strong Control and User Satisfaction in Business Mobility,” n.d.). Using personal smartphones, tablets, or laptops for work introduces security, data management, and device compatibility complexities. Challenges arise from the diverse nature of individual devices, potentially compromising organizational security and data integrity. Implementing well-defined policies and robust security measures to regulate BYOD usage becomes essential to mitigate potential risks. This involves setting clear guidelines on permissible devices, establishing security protocols, and ensuring device compatibility with organizational systems. Furthermore, educating employees on BYOD best practices is vital for fostering awareness about potential security risks and promoting responsible device usage.

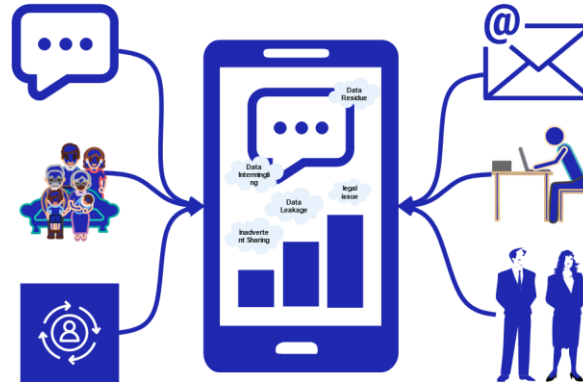


Fig. 1 Coexistence of personal and work data

B Privacy Risks with Coexistence of Personal and Work Data

Privacy risks arising from the coexistence of personal and work data on the same device present significant concerns for organizations (Tairov et al., 2016). A visual representation is shown in Fig. 1. The intermingling of these data types can lead to accidental mixing of files, potential leakage between personal and work-related apps, inadvertent sharing with colleagues or external parties, and the persistence of data residue even after deletion. The risk intensifies in the event of device loss or theft,

where sensitive information may be compromised. Legal and compliance issues may arise, mainly concerning personal data privacy regulations. User awareness and training are crucial to addressing these risks effectively, emphasizing the importance of data segregation and the potential consequences of inadequate privacy practices (Singh, 2022).

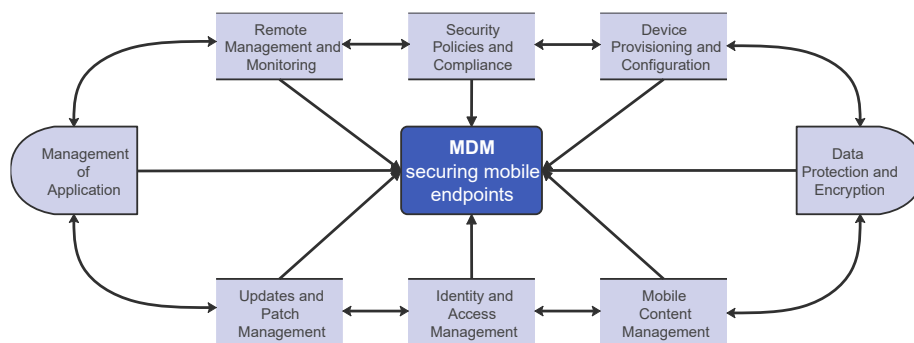
C Balancing Convenience with Security

Balancing convenience with security in the dynamic world of mobile endpoints is crucial for organizations seeking to optimize productivity while safeguarding sensitive information (Tairov et al., 2016). One challenge lies in implementing user-friendly security measures that enhance protection without impeding user workflows. Context-aware policies offer a solution, allowing organizations to tailor security measures based on location, network, and device type, fostering flexibility when appropriate. Educating and raising awareness among users about security best practices address the challenge of inadvertent compromises due to a lack of knowledge. Risk-based approaches involve assessing device health and user behavior and applying suitable security controls to high-risk scenarios.

MDM IN SECURING ENDPOINTS

MDM is pivotal in managing and securing various endpoints, including smartphones, tablets, and laptops. Employed as a method to centrally manage, control, and secure data and information across an organization, MDM effectively tackles challenges related to data security, device management, and compliance for mobile endpoints [Sisala and Othman, 2020c] [Shin et al., 2008]. The aspects of securing endpoints are shown in Fig. 2.

Fig. 2 MDM in securing mobile endpoint security



1. Device Provisioning and Configuration: MDM empowers organizations to provision and configure mobile devices standardized and securely. This involves establishing device settings, network configurations, and security policies before deploying devices to end-users.

1. **Security Policies and Compliance:** MDM enables enforcing security policies on mobile devices. This includes setting password requirements, configuring encryption, and imposing restrictions on specific device functionalities. Compliance with regulatory standards and organizational security policies can be consistently maintained across all endpoints.
2. **Remote Management and Monitoring:** MDM allows IT administrators to monitor and manage mobile devices remotely. This includes tracking device location, monitoring device health, and troubleshooting issues without physical access. Remote management capabilities enhance efficiency and reduce the need for on-site support.
3. **Application Management:** MDM facilitates the distribution and management of applications on mobile endpoints. IT administrators can control which applications are allowed or prohibited, ensuring that only authorized and secure applications are installed on devices.
4. **Data Protection and Encryption:** MDM helps implement data protection measures, such as encrypting sensitive data stored on mobile devices. This is crucial for preventing unauthorized access to confidential information if a device is lost or stolen.
5. **Identity and Access Management:** MDM integrates with identity and access management systems to ensure only authorized users can access corporate resources. This helps in preventing unauthorized access and data breaches.
6. **Mobile Content Management:** MDM solutions often include features for managing and securing corporate content on mobile devices. This includes remotely wiping corporate data from a device and ensuring that sensitive information does not fall into the wrong hands.
7. **Updates and Patch Management:** MDM assists in keeping mobile devices up to date with the latest software patches and updates. This is critical for addressing security vulnerabilities and ensuring that devices are running on the most secure and stable versions of their operating systems and applications.

PROPOSED DUAL USER-BASED MDM SOLUTION

In this study, we propose a dual user-based solution for Mobile Device Management (MDM), leveraging the existing dual-user options available in modern smartphones as depicted in Fig. 3. This approach allows users to have two distinct profiles on their phones, one for personal use and the other for work-related activities, akin to having

two separate devices. The proposal includes implementing a unified notification panel that enables users to seamlessly access notifications from both profiles (Wang et al., 2014a).

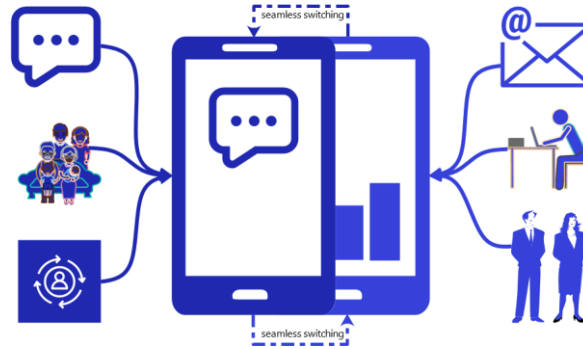


Fig. 3 Proposed Dual User-Based MDM Solution

A Strengths

Enhanced Security: Separating personal and work data into distinct profiles minimizes the risk of data breaches and unauthorized access. Sensitive work data remains isolated from personal apps and activities. **Improved Productivity:** Clear delineation between work and personal life reduces distractions, promoting focused work during dedicated work hours. **Flexibility and Convenience:** Users can seamlessly switch between profiles, accessing work notifications and apps without impacting personal usage. **Hardware Compatibility:** Many mid-tier to high-end phones already offer dual-user features, making hardware feasibility a non-issue.

B Challenges

Software Integration: Seamless integration with existing MDM solutions and notification systems might require software development or customization. **User Adoption and Education:** Encouraging users to adopt and utilize dual profiles requires clear communication, training, and ongoing support.

C Hardware and Software Considerations

Hardware Capabilities: Evaluate different phone models' specific dual-user features and limitations to ensure compatibility and optimal performance. **Software Development:** Explore existing MDM solutions that support dual user profiles or consider custom development to integrate seamlessly with your desired functionality. **Security Testing:** Rigorously test the security of the dual-user system to identify and address any potential vulnerabilities. **User Experience Design:** Design an intuitive and user-friendly interface for profile switching, notification access, and data management within the dual-user environment.

PROPOSED MDM IMPLEMENTATION

This section provides a comprehensive life cycle methodology designed to embed security considerations throughout deploying enterprise mobile device solutions. The approach is organized into five distinct phases, each catering to specific tasks and considerations relevant at different stages of the mobile device solution life cycle.

A Phase 1: Initiation

The initiation phase initiates the life cycle by addressing tasks preceding the design of the mobile device solution. This involves identifying organizational needs for mobile devices, establishing a vision aligning mobile solutions with the organizational mission, formulating a high-level implementation strategy, crafting a robust mobile device security policy, and specifying business and functional requirements for the solution.

B Phase 2: Development

During the development phase, personnel articulate the technical characteristics of the mobile device solution. This includes specifying authentication methods and cryptographic mechanisms and determining authorized types of mobile devices. The focus is on ensuring alignment with security policies, enabling the practical application and enforcement of the mobile device security policy. This phase concludes with the procurement of solution components based on specified requirements. Fig. 4 shows the steps in detail.

C Phase 3: Implementation

Equipment is configured to meet operational and security requirements in the implementation phase. This involves translating the mobile device security policy into actionable configurations documented in the system security plan. The solution undergoes installation and testing as a pilot before activation on a production network. Integration with other security controls and technologies, such as event logging and authentication servers, is integral to this phase.

D Phase 4: Operations and Maintenance

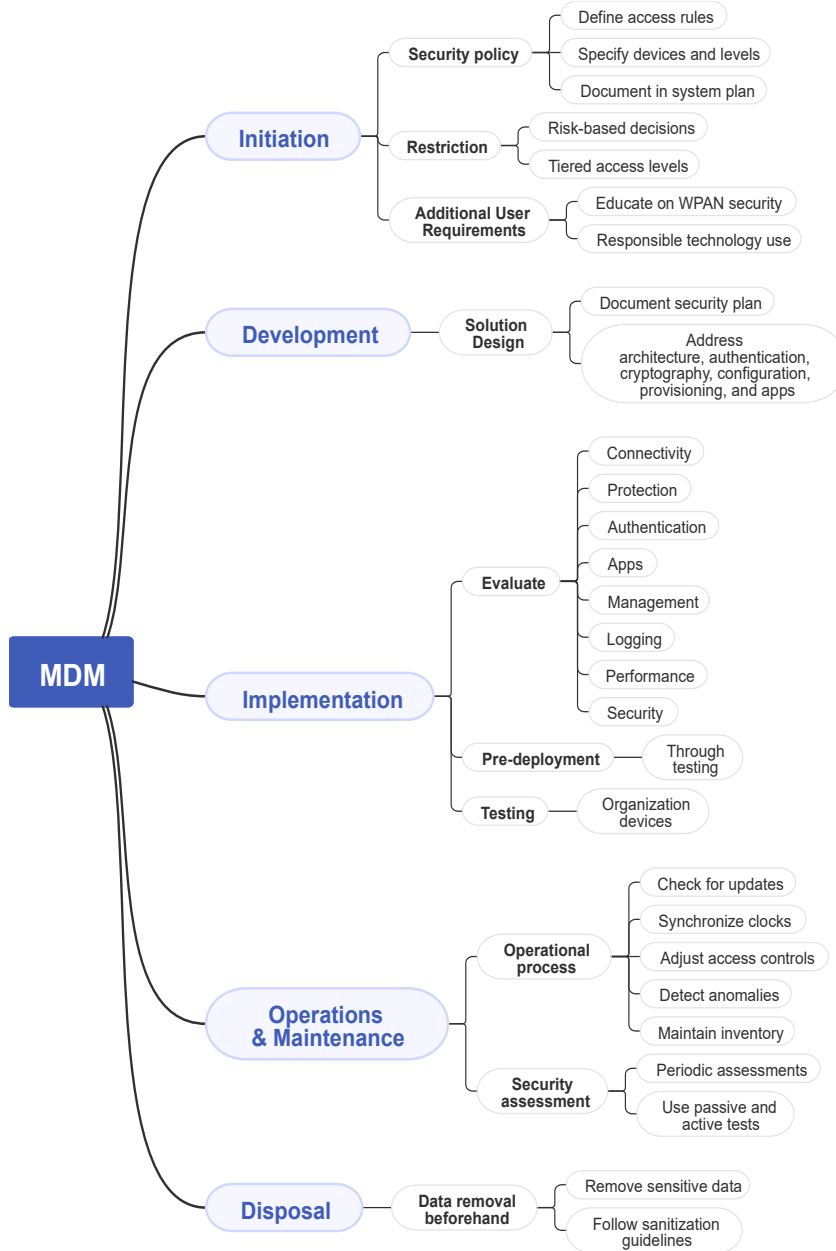
Phase 4 focuses on ongoing security-related tasks when the mobile device solution is operational. Regular patching, periodic log reviews, and continuous monitoring are vital to address vulnerabilities, monitor system activity, and detect potential security incidents, ensuring sustained security posture.

E Phase 5: Disposal

The disposal phase manages tasks associated with retiring the mobile device solution or its components. This includes preserving information for legal requirements, sanitizing media for secure data removal, and disposing of equipment properly adhering to established security and environmental protocols.

Organizations can tailor this life cycle model to align with their project management methodologies, fostering a consistent and comprehensive approach to mobile device security throughout the solution's life cycle.

Fig. 4 Life cycle implementation process



BENEFITS OF THE PROPOSED MDM

Mobile Device Management (MDM) is instrumental in fortifying an organization’s security posture by providing a comprehensive suite of features that explore data security and malware protection, ensuring robust defense against potential threats.

A Data Security

a Preventing Unauthorized Access:

MDM is a vigilant guardian, implementing stringent measures to ensure that only authorized users can access corporate data on mobile devices. The multifaceted approach involves the following key features:

- **Device Enrollment:** MDM facilitates secure onboarding, ensuring only authorized devices can access corporate resources.
- **User Authentication:** Strong user authentication mechanisms, including biometrics or multi-factor authentication, add a layer of security.
- **Role-Based Access Controls (RBAC):** RBAC allows administrators to define specific roles and permissions, ensuring that users only access the data and functionalities necessary for their roles.

Unauthorized users are systematically restricted from accessing sensitive information, actively reducing the risk of data breaches and unauthorized access.

b Remote Wipe:

MDM provides a critical countermeasure by implementing remote wipe capabilities in the unfortunate event of device loss or theft. This feature empowers administrators to remotely erase corporate data from the device, preventing unauthorized access to confidential files. For example, if an employee's phone is stolen, the IT team can initiate a remote wipe, ensuring the swift and secure removal of all work-related data.

c Encryption:

MDM solutions enforce robust encryption protocols for data at rest and in transit. This ensures that the encrypted data remains unreadable even if a device falls into the wrong hands. Centralized management of encryption keys adds a layer of security, enhancing the protection of sensitive information.

d Access Controls:

MDM enables administrators to exert granular control over app access and permissions. This involves defining specific conditions under which apps can access corporate data. For instance, sensitive apps may require multi-factor authentication, adding an extra layer of security to critical data and applications.

B Malware Protection

a Minimizing Malware Risk:

MDM solutions include robust features designed to detect and prevent malware, providing a multi-faceted approach to minimize the risk of malicious attacks:

- **Regular Scans:** MDM conducts regular scans of devices to identify and quarantine potentially harmful apps or files.
- **Real-Time Monitoring:** Continuous real-time monitoring immediately identifies suspicious behavior, triggering prompt actions to prevent malware proliferation.

By promptly blocking or quarantining infected devices, MDM actively mitigates the risk of malware spreading within the organization.

b Security Updates:

MDM adopts a proactive stance in ensuring that devices receive timely security patches and updates. This involves:

- **Timely Distribution:** MDM ensures the timely distribution of security patches to all enrolled devices.
- **Vulnerability Management:** Regular updates protect against emerging threats and vulnerabilities, addressing known security flaws in operating systems and applications.

MDM provides a proactive defense against evolving security threats by constantly updating devices, bolstering the organization's overall security resilience.

CONCLUSION

This study explores the multifaceted landscape of Mobile Device Management (MDM) and proposes a novel approach to enhance security and user experience through dual user profiles. Integrating MDM solutions in securing enterprise mobile devices is critical for maintaining data integrity, enforcing security policies, and mitigating potential threats. The proposed dual-user-based MDM solution leverages the capabilities of modern smartphones that offer dual-user options (Zefferer & Teufl, 2013). The solution aims to enhance security, productivity, and user flexibility by providing distinct profiles for personal and work use. The strengths of the proposed model lie in its ability to separate sensitive work data from individual activities, promote focused work hours, and seamlessly switch between profiles. The compatibility with mid-tier to high-end phones addresses hardware concerns while acknowledging the need for software improvements .

However, challenges such as software integration, user adoption, and potential security gaps necessitate careful consideration. Clear communication, training, and ongoing support are crucial for encouraging users to utilize dual profiles effectively. Security testing and software development may be required to integrate the proposed solution seamlessly with existing MDM systems. The life cycle implementation methodology presented in this study provides organizations with a structured approach to incorporating security throughout the entire life cycle of enterprise mobile device solutions. From initiation to disposal, each phase emphasizes the importance of addressing security concerns and ensuring compliance with organizational and regulatory standards.

REFERENCES

- Batool, H., & Masood, A. (2020). Enterprise Mobile Device Management Requirements and Features. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 109–114.
- Jalili, M. (2014). *Analyse Mobile Device Management Criteria*. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:763990>
- Singh, J. P. (2022). Mitigating Challenges in Cloud Anomaly Detection Using an Integrated Deep Neural Network-SVM Classifier Model. *Sage Science Review of Applied Machine Learning*, 5(1), 39–49.
- Singh, J. P. (2023). Enhancing Database Security: A Machine Learning Approach to Anomaly Detection in NoSQL Systems. *International Journal of Information and Cybersecurity*, 7(1), 40–57.
- Sisala, S., & Othman, S. H. (2020). Developing a Mobile Device Management (MDM) security metamodel for bring your own devices (BYOD) in hospitals. *International Journal of Innovative Computing*, 10(2). <https://doi.org/10.11113/ijic.v10n2.273>
- Solutions to a Balanced Approach between Strong Control and User Satisfaction in Business Mobility. (n.d.). In *Proceedings of International Conference on Application of Inf.*
- Tairov, Popov Tairov, I., & Popov, V. (2016). Solutions to a Balanced Approach between Strong Control and User Satisfaction in Business Mobility. In *Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE)* (pp. 324–329).

Wang, Y., Wei, J., & Vangury, K. (2014a, January). Bring your own device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*. 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV. <https://doi.org/10.1109/ccnc.2014.6866552>

Wang, Y., Wei, J., & Vangury, K. (2014b). Bring your own device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, 80–85.

Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 143–147.

Zefferer, T., & Teufl, P. (2013). Policy-based security assessment of mobile end-user devices an alternative to mobile device management solutions for Android smartphones. *2013 International Conference on Security and Cryptography (SECRYPT)*, 1–8.