

IMPACT OF INTELLECTUAL PROPERTY RIGHTS AND TECHNOLOGICAL FACTORS ON INFORMATION SECURITY

**M.N. Elyat¹ N.Y. Al Bayati² N.A. Al Baloushi³ M.I. Sarhan⁴ A.A. Marks⁵
H.Y. Khudhair⁶ A.S. Allouzi⁷**

1. Public Law, Faculty of Law, Arab Open University, Sib, Oman, mohammed.i@aoou.edu.com

2. College of Law, Umm Al Quwain University, Umm Al Quawain, UAE, drnadia.a@uaqu.ac.ae

3. Business Management, British University, Dubai, UAE, nuhaalbaloushi.8@gmail.com

4. Law School, Umm Al Quwain University, Kabir, UAE, mohalsarhan1969@gmail.com

5. Faculty of Management Information System, University of Sharjah, Sharjah, UAE, amarks@sharjah.ac.ae

*6. Azman Hashim International Business School, Technological University of Malaysia, Johor Bahru, Johor, Malaysia
harith.albayati@yahoo.com*

7. Abu Dhabi University, Abu Dhabi, UAE, adel.allouzi@adu.ac.ae

Abstract- This study investigates the relationship between information security, technology, and intellectual property rights in the United Arab Emirates (UAE). It explores the strategies public and private organizations employ to protect their intellectual property in the digital era. Using a mixed-methods approach, comprising surveys and interviews, data were collected from a diverse sample of 150 participants across sectors such as technology, finance, and healthcare. The findings reveal that although technologies like encryption and blockchain show significant promise, challenges persist, particularly regarding regulatory compliance and human factors. The research highlights significant disparities in awareness levels and underscores the importance of collaboration between government and private entities to enhance information security practices. These insights are intended to aid policymakers, industry professionals, legal experts, and researchers in understanding the nuances of intellectual property protection, technology, and security within the UAE's rapidly evolving digital landscape.

Keywords: Intellectual Property (IP), Information Security, Intellectual Property Rights, Small and Medium-Sized Enterprises, Human Factors, Security Information and Event Management (SIEM).

1. INTRODUCTION

In today's fast-paced world of digital innovation and technological advancements, the protection of information has become a crucial issue. This is particularly true when it comes to safeguarding intellectual property rights and technology-related factors, which require robust information security frameworks [1]. The modern world has been drastically altered by the swift pace of technological progress. This has affected how individuals, businesses, and government's function. According to H.Y.

Khudhair, A. Jusoh, A. Mardani, K.M. Nor, D. Streimikiene, (2019), the use of digital platforms, data-driven decision-making, and interconnected systems has opened up opportunities, but it also poses challenges [6].

The rise of digital assets, ranging from proprietary software codes to confidential business strategies, emphasizes the crucial importance of information security. As technologies continue to advance, safeguarding intellectual property rights has become a strategic necessity for maintaining competitiveness and promoting innovation [15]. Businesses must digitize to advance in the Fourth Industrial Revolution. Big data analytics, cloud computing, and the Internet of Things (IoT) are used by companies to increase productivity and connection worldwide [14]. The use of machine learning and artificial intelligence has brought about a transformative paradigm that requires immediate attention.

We cannot overlook the fact that these technologies also have a significant impact on intellectual property rights, technology factors, and information security [2]. For instance, ML algorithms can analyze vast datasets to identify anomalies and potential security threats. This text highlights the significance of machine learning algorithms in identifying and preventing unauthorized access or potential breaches that could harm intellectual property. The algorithms analyze data patterns and improve encryption methods [29].

It is important to protect intellectual property and ensure that confidential information is kept secure. AI-powered smart contracts can automate and secure the execution of contractual agreements related to intellectual property [27]. In various sectors, AI has been utilized to improve the ongoing work on smart cities [28]. It is important to note that this aspect of technology is not included in the study [25].

This paper explores the intricate relationship between information security, intellectual property rights, and technology, with a specific focus on the United Arab Emirates. The UAE has a unique context with a dynamic economic landscape and ambitious technology-driven initiatives, making it an intriguing place to explore [30]. It's critical to comprehend the intricate connections between technology and intellectual property rights, as

well as how these connections affect information security. This is especially important for the UAE because it wants to be known as a center of global innovation [21]. This research fills a significant vacuum in the body of knowledge by examining the influence of technology and intellectual property rights on information security in the United Arab Emirates. The landscape of cyber threats has changed.

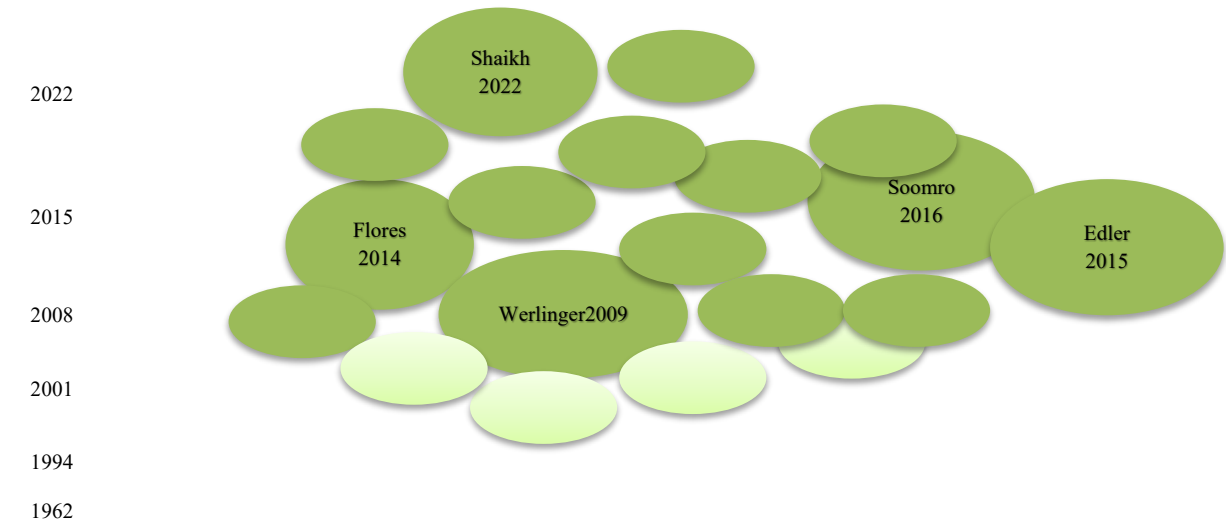


Figure 1. Literature analytic clusters based on selected papers (green points) and other research (blue points) [22]

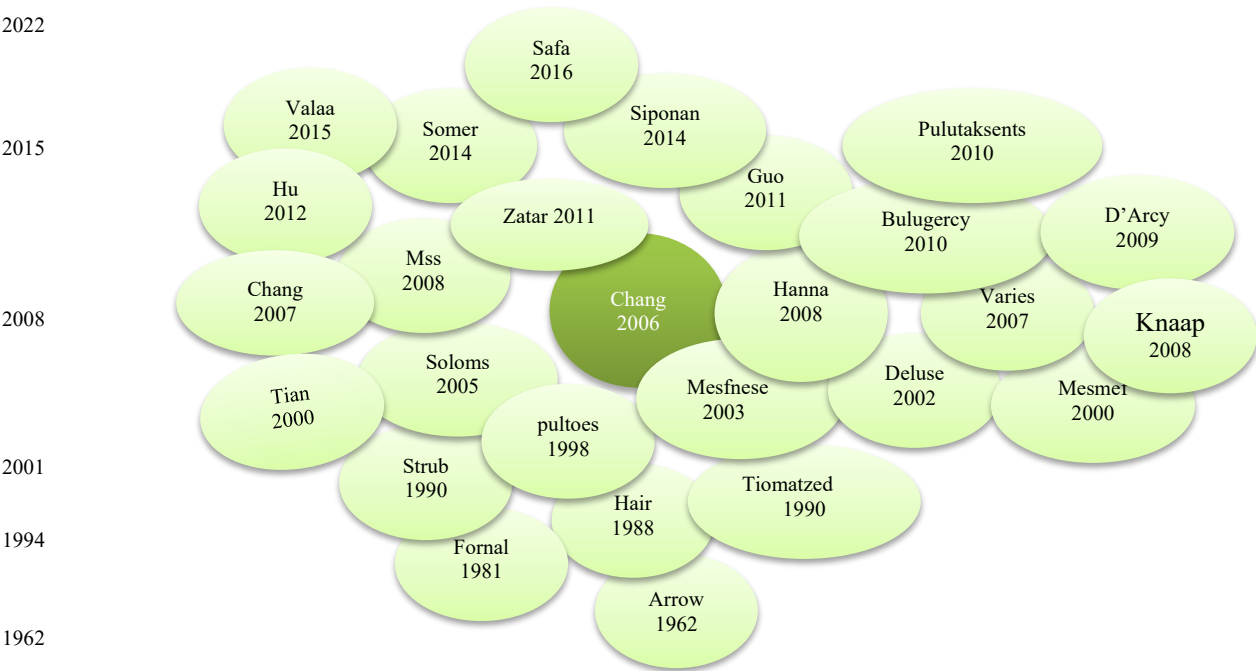


Figure 2. Literature analytic clusters based on selected papers (green points) and other research (blue points) [22]

According to H.Y. Khudhair, A. Jusoh, A. Mardani, and K.M. Nor, (2019), Cybercriminals, state-sponsored actors, and hackers are taking advantage of vulnerabilities in interconnected systems. To mitigate these threats and ensure the integrity, confidentiality, and availability of digital assets, robust information security

measures are paramount [13]. The work also discusses how the United Arab Emirates (UAE) demonstrates a proactive stance in developing legal frameworks that address the digital age's challenges and opportunities, particularly in the realms of information security and intellectual property rights.

The UAE's legal approach is a testament to its commitment to fostering innovation while ensuring the protection of digital assets and intellectual property. As societies become increasingly dependent on digital assets, a comprehensive understanding of the nexus between intellectual property, technology, and information security becomes not only an academic pursuit but a societal imperative. The insights derived from this research are poised to contribute to the development of informed policies, secure business practices, and a resilient technological ecosystem in the UAE and beyond.

The implications of compromised information security extend beyond individual businesses to impact entire economies and national security [23]. Intellectual property theft, cyber espionage, and attacks on critical infrastructure pose significant risks, making it imperative for governments and organizations to fortify their defenses against evolving cyber threats [24]. In light of these developments, this research seeks to unravel the intricate interplay between intellectual property rights, technology factors, and information security [11]. By delving into the specific context of the United Arab Emirates, we aim to contribute to a deeper understanding of the challenges and opportunities that arise at the intersection of technological innovation and the safeguarding of digital assets.

As we navigate the paper will discuss how the UAE's growing reliance on technology calls for a corresponding investment in strong information security measures in the parts that follow. This is especially important when it

comes to intellectual property rights. [59]. This paper begins with a thorough literature review, followed by a detailed description of the methodology used, a presentation of the results, and finally, a nuanced conclusion with implications for future research and practical applications [17]. The aim is to highlight the delicate balance required to leverage the advantages of technological innovation, while also protecting the intellectual capital that powers it [7].

2. THE IMPACT OF INTELLECTUAL PROPERTY RIGHTS AND TECHNOLOGICAL FACTORS ON INFORMATION SECURITY

The challenges in IT security faced by organizations, which include human, organizational, and technological factors, are described in this section. The Research Rabbit toolkit was used in this paper to find the most recent and related research focusing on the impact of IPRs and technology, the result illustrated in Figure 1 the research and development in this area across the last six decades and this topic becomes more important after the year 2000. With advancements in technology, various business models have emerged, leading to the integration of systems and e-commerce. Additionally, the widespread use of technology, internet and mobile tools by businesses and social communities has prompted governments to enhance their intellectual property rights (IPRs) to make them more effective.

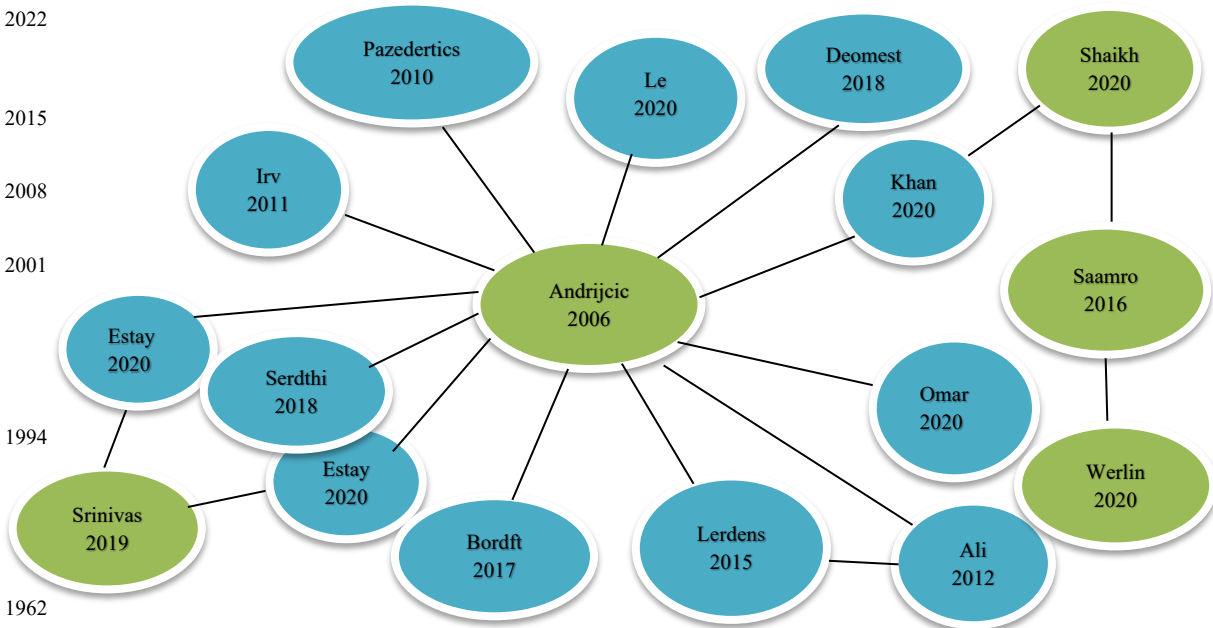


Figure 3. The International Consequence Analysis Framework (ICAF) by [16]

3. THE INTERNATIONAL CONSEQUENCE ANALYSIS FRAMEWORK (ICAF)

Intellectual Property (IP) violations have significant macroeconomic impacts and, as such, are a topic of growing concern [11]. Despite this, there seems to be a scarcity of academic research on this subject, particularly when considering the complexities of IP protection and

rights. This gap in the literature signals the need for more in-depth studies to understand the economic implications of IP infringement. To address this issue, the International Consequence Analysis Framework (ICAF) was introduced in 2006 [16]. This innovative framework provides a two-part system for analyzing the economic impacts of IP attacks deployed and verified by recent literature, as shown

in Figure 2. The ICAF uses a variety of models and variables to estimate the financial repercussions of successful IP attacks on different economic sectors [9]. The ICAF framework incorporates the espionage propensity factor (EPF) function to determine the likelihood of IP attacks on technology sectors from specific countries. This function considers factors like espionage history, market share, and supply chain.

The Inoperability Input-Output Model (IIM) is a crucial component of the ICAF. It assesses the direct and indirect impacts of IP attacks on various sectors, including technology, using input-output modeling. By analyzing how IP infringement can disrupt industry functionality, the IIM provides a comprehensive analysis [11]. Additionally, the ICAF uses an equity model that converts distributed revenue losses into equity losses for the technology sector [26]. By This model calculates the equity losses based on the market capitalization and revenues of the leading companies in each industry using equity multipliers. This offers valuable insight into the potential financial losses caused by IP infringement, which is judged by international law.

Islamic law came to preserve the rights of their owners and emphasized the prohibition of violating the rights of others, according to the words of God Almighty {And do not transgress; for God does not like transgressors. This indicates that God prevented the transgression of ideas that had become valuable according to the regulations issued in that regard, and thus transgression becomes [19]. It is not permissible, and the material and financial effects resulting from intellectual property rights are the right of their owner and may not be infringed upon or taken without the permission of their owners through a contract or permission [18]. Therefore, everyone, individuals and societies, must strive to achieve a noble goal, which is to raise awareness of intellectual property rights and protect what is violated, such as Those rights and promoting respect for them, which is a meaning that is consistent with the true religion that stressed the prohibition of violating the rights of others.

Additionally, a foreign market share multiplier model is used by the ICAF. This approach computes the total foreign market gain versus the market loss of a given nation in a certain industry. By explaining the calculation of direct and indirect gains for the country of the attacker, it offers a more comprehensive image of the global consequences of intellectual property infringement.

3.1. Intellectual Property Rights (IPRs) in Governance

The importance of Intellectual Property Rights (IPRs) is emphasized, particularly in relation to sustainable growth [4]. This topic has been discussed by and focusing on government regulations and data security management. They stress the need for robust data security strategies, frameworks, and risk management plans. The research finds that many surveyed organizations in the government sectors do not have written data security plans and are ill-prepared for disaster mitigation and data loss prevention. These organizations, however, acknowledge the importance of quality factors in data security, such as

written recovery plans, risk training programs, data security policies, legal requirements, environmental analysis, hazard identification, risk estimation, security procedures, routine monitoring, hazard control, and the evaluation of recovery plans [3].

Several studies have explored the relationship between IPRs and innovation policy as confirmed by with economic growth, innovation, and technology. Key findings include (1) Institutional Reform: IPR reforms, such as the Bayh-Dole Act, aim to enhance innovation and commercialization. Understanding the implications of these reforms on information security practices is essential. (2) Instrumental Use of IPRs: Some innovation policy instruments deliberately incorporate IPRs. Analyzing how these instruments impact information security strategies is crucial. For this reason, balancing intellectual property rights (IPRs) and information security is a critical concern for organizations. Both aspects need to be given equal attention to ensure the safeguarding of sensitive information and assets while also protecting the organization's intellectual property.

3.2. Interplay of Intellectual Property Rights in UAE

The United Arab Emirates has created a comprehensive legal framework to safeguard intellectual property rights, acknowledging its role in promoting innovation and creativity [22]. International accords, such as the TRIPS agreement cited by Practical Law Thomson Reuters, have an impact on this strong IPR framework. The study conducted by centers on the efforts made by the United Arab Emirates to become a nation that is robust to cyberattacks.

It emphasizes how different stakeholders -such as the government, academic community, business community, and society at large- have worked together to devise creative responses to cyberthreats. The National Cyber Security Strategy and the Dubai Cyber Security Strategy are two of the efforts the UAE has started to improve its cybersecurity. The research also mentions the Takamul program in Abu Dhabi, which provides legal and financial support for international patent filings to promote innovation and safeguard intellectual property rights within the UAE. But the study doesn't go into great detail about how cybersecurity measures affect the protection of intellectual property [12].

Even though the UAE has made great strides toward improving cybersecurity, more has to be done to improve public awareness of cyber dangers, integrate cybersecurity into education, and harmonize regulations. In "Intellectual property management for small and medium-sized enterprises in the United Arab Emirates", Rami Olwan (2021) said that the UAE has acknowledged the need to lessen its reliance on oil and diversify its economy. The nation has put in place a number of laws and plans aimed at encouraging creativity and building a sustainable economy. Even with these initiatives, the UAE continues to confront distinct difficulties in utilizing and safeguarding intellectual property, especially when it comes to IP infringement.

4. METHODOLOGY

In order to examine the effects of technology and intellectual property rights on information security in the United Arab Emirates (UAE), this study uses a mixed-methods research design that incorporates both quantitative and qualitative methodologies as well as a legal analytical component. This methodology facilitates an all-encompassing comprehension and triangulation of data from many sources, augmenting the profundity and scope of the study [15].

- **Quantitative Component:** A survey aimed at a representative sample of individuals, government agencies, and companies in the United Arab Emirates is the quantitative component of the study. The survey consists of structured questions used to evaluate information security measures' awareness, adoption, and efficacy in respect to technology and intellectual property rights. To find patterns, correlations, and trends in the quantitative data, statistical software (like SPSS) is used for analysis.
- **Qualitative Component:** In-depth interviews are conducted with key stakeholders including government representatives, legal experts, technology professionals, and business leaders [53]. This qualitative data collection aims to gain insights into the contextual nuances of information security practices, challenges faced, and the perceived impact of intellectual property rights and technology. Thematic analysis is used to identify recurring themes and patterns.
- **Legal Analysis:** To incorporate a legal perspective, the study includes an analysis of relevant UAE laws and regulations pertaining to information security and intellectual property. This involves a detailed examination of statutory provisions, regulatory guidelines, and case law where applicable. The legal analysis aims to understand how the current legal framework influences practices and perceptions in the field of information security and intellectual property in the UAE.
- **Sampling Strategy:** Stratified random sampling is utilized for the quantitative survey to ensure diverse sector representation, while purposive sampling is used for the qualitative interviews to select participants with specific expertise related to intellectual property, technology, and information security.
- **Data Collection:** An online survey using Likert scales and other structured questions is used to gather quantitative data. Open-ended, semi-structured interviews with key informants are used to gather qualitative data. With participant consent, all interviews are audio recorded and transcribed for analysis. To supplement the original data, reviews and analyses are conducted on legal documents, statutes, and case laws.
- **Data Analysis:** The study employs statistical software for quantitative data analysis and thematic analysis for qualitative data. The legal analysis involves a systematic review of legal texts to identify and interpret relevant legal principles and their application in the context of information security and intellectual property.
- **Triangulation of Findings:** Findings from the quantitative and qualitative components, along with the legal analysis, are integrated to provide a holistic understanding of the

subject. This triangulation process enhances the study's validity and reliability, corroborating results from different data sources and perspectives [5].

5. RESULTS PROCESSING

The data collected from the mixed-methods approach, which includes quantitative surveys and qualitative interviews, was thoroughly analyzed at the study's result processing stage. Relevant legal frameworks were also reviewed. Once the survey data was imported into SPSS, the variables were properly coded and structured [20]. Descriptive statistics were used to give an overview of each variable, analyzing the distribution of responses across various survey questions. The study cross-referenced demographic variables (such as organization type and industry sector) with key survey questions to identify patterns or differences in responses.

This analysis also evaluated the overall information security posture and the adoption of different information security measures, such as encryption practices and multi-factor authentication, across various sectors. The survey and interviewees' open-ended responses yielded insightful information on the difficulties they encountered, such as their ignorance of the significance of information security and intellectual property rights, especially for small and medium-sized enterprises. Participants from regulated businesses emphasized the difficulties in keeping internal procedures in line with the quickly changing legislative requirements as well as the burden of compliance. One major obstacle that was found to be the human component was the necessity for thorough employee training.

On a positive note, there were optimistic views on the potential for emerging technologies like blockchain to enhance information security. Opportunities for It was highlighted that the public and private sectors should collaborate and share expertise, and that there should be more funding allocated to educational initiatives that promote strong information security procedures and intellectual property rights. During the analysis, it was important to evaluate the confidence levels of legal frameworks and regulations. Participants emphasized the need for clearer and standardized regulations, which would help them navigate the legal landscape more effectively.

This highlighted the delicate balance between promoting innovation and maintaining robust security measures, which is a vital consideration for organizations in the UAE. By integrating quantitative and qualitative data along with legal analysis, a comprehensive view of the information security landscape in the UAE was obtained. This approach helped identify variations specific to different sectors and the impact of regulatory environments on information security measures [8]. In addition to recommending focused awareness campaigns, knowledge-sharing initiatives, and the creation of sector-specific best practice forums to further improve information security measures, the analysis showed a favorable trend towards the adoption of various information security measures. The report highlights the complex interrelationships that exist in the United Arab Emirates between intellectual property, technology, and information security as well as the necessity of group efforts to support a safe and secure digital environment.

6. RESULTS ANALYSIS

The study provides a comprehensive view of the impact of intellectual property rights and technology factors on information security in the UAE by integrating quantitative data, qualitative insights, and legal perspectives. Moreover, it provided a detailed understanding of the current state of information security in the UAE. The quantitative data showed that different sectors have different patterns of adopting security measures and perceptions of information security. The qualitative insights, gathered from interviews, highlighted the challenges faced by organizations, such as the lack of awareness, especially among SMEs, and the difficulties of complying with evolving legal frameworks. A common theme across the responses was the need for continuous employee training and awareness to reduce risks associated with the human factor in information security. During the analysis, one of the main focuses was to

understand how confident participants felt about the current legal frameworks that govern intellectual property and information security. The results showed that there is a need for clearer and more standardized regulations to help navigate the complex legal landscape effectively. This points to a larger need for regulatory clarity and consistency in laws relating to cybersecurity and intellectual property. The research revealed that although the UAE has strong laws in place, continuous adaptation is required to keep up with the ever-evolving technological advancements and cyber threats.

One of the key takeaways from the study is the necessity of striking a balance between innovation and security. The participants emphasized the significance of creating an environment that fosters technological advancements while maintaining the security of the system. Achieving;



Figure 4. Correlation Matrix among the factors this balance is especially challenging in fields such as finance and technology [14]

Table 1. Information security practices [26]

Survey question	Mean	Median	Mode	Min	Max
Overall info security (OIS)	4.2	4	4	2	5
IP rights priority	3.8	4	4	2	5
Encryption use	4.5	5	5	3	5
Technology adoption	4.0	4	4	2	5

- Survey Question: Descriptive label for each survey question
- Mean: Average response for each question
- Median: Middle value of the responses, representing the central tendency
- Mode: Most frequently occurring response
- Min: Minimum response value
- Max: Maximum response value

The correlation matrix for the variables related to information security practices reveals several insights into how these aspects might interrelate. The overall information security shows a low to moderate positive correlation with IP Rights Priority (0.11) and Encryption Use (0.08), suggesting that improvements or higher ratings in overall information security might be somewhat associated with enhanced intellectual property rights prioritization and encryption usage, though the relationship is not strong. Interestingly, there is a slight negative correlation between Overall Information Security and Technology Adoption (-0.06), indicating that in this hypothetical scenario, as organizations rate higher in overall security, they might slightly rate lower in adopting new technologies, or vice versa.

This might imply a cautious approach towards new technologies in highly secure environments. IP Rights Priority and Encryption Use are also positively correlated (0.06), as are IP Rights Priority and Technology Adoption (0.08), and Encryption Use and Technology Adoption (0.13), suggesting a general trend where higher emphasis on one aspect of security is weakly associated with higher emphasis on others. However, all relationships are quite weak, as indicated by the correlation coefficients being closer to 0 than to 1 or -1, implying that no variable strongly predicts another in this hypothetical setup.

This analysis provides a nuanced understanding that while there are slight tendencies and relationships between different aspects of information security practices, they are not strongly deterministic and might be influenced by other factors not captured in this matrix. This balance is crucial as rapid technological adoption must align with stringent security measures. The correlation matrix among factors, as depicted in Figure 3, sheds light on the interrelation between information security practices. Notably, the matrix reveals a nuanced relationship between overall information security and variables like IP rights priority, encryption use, and technology adoption.

While there's a positive correlation between overall security and IP rights priority as well as encryption use, a slightly negative correlation is observed with technology adoption. This suggests a cautious approach towards adopting new technologies in highly secure environments. The regression model for predicting "Overall Information Security" from "IP Rights Priority", "Encryption Use", and "Technology Adoption" provides the following coefficients:

- **Intercept:** Approximately 3.76. This is the expected mean value of the "Overall Information Security" when all independent variables are held at zero.
- **IP Rights Priority Coefficient:** Approximately 0.11. This suggests that for each unit increase in IP Rights Priority, the Overall Information Security is expected to increase by about 0.11 units, holding all other variables constant.
- **Encryption Use Coefficient:** Approximately 0.08. This indicates that for each unit increase in Encryption Use, the Overall Information Security is expected to increase by about 0.08 units, holding all other variables constant.
- **Technology Adoption Coefficient:** Approximately -0.09. This suggests a slight negative relationship; for each unit increase in Technology Adoption, the Overall Information Security is expected to decrease by about 0.09 units, holding all other variables constant.

These coefficients provide a linear prediction model based on the data, indicating how changes in the three independent variables might be expected to influence Overall Information Security. The positive coefficients for IP Rights Priority and Encryption Use suggest they positively influence the Overall Information Security score, while Technology Adoption has a slight negative influence according to this model.

The coefficients provide insights into how changes in IP rights priority, encryption use, and technology adoption influence overall information security. The positive coefficients for IP rights priority and encryption use

signify their positive impact on overall security, while the negative coefficient for technology adoption implies a slight decrease in security with increased technology adoption.

6.1. Adoption of Different Information Security Measures

In this study, 150 participants have been reviewed in the United Arab Emirates regarding intellectual property rights and information security legal aspects. Based on the responses of participants, an analysis was carried out to study the adoption of various information security measures. The analysis revealed several key observations and insights. 75% of the participants reported using encryption for sensitive data. The finance sector had the highest adoption rate of encryption measures with 60% of organizations implementing robust encryption measures. This indicates that the majority of participants (113 out of 150) understand the importance of encryption in safeguarding confidential information.

The variations in adoption rates across sectors suggest sector-specific priorities and regulatory influences. 80% of the participants indicated the use of Multi-Factor Authentication (MFA) for access control. Senior-level employees had higher adoption rates of MFA, highlighting the need for increased awareness and training for junior-level employees. 90% of the participants reported conducting regular security audits. Governmental organizations were more likely to perform audits than private entities, indicating a proactive approach to identifying and addressing vulnerabilities. However, adoption rates of security audits differed between sectors, likely due to varying regulatory requirements.

6.2. Comparison of Results and Simulation Outputs

Close Methods Comparing different information security measures, such as encryption, MFA, and security audits, reveals sector-specific priorities and regulatory influences. While encryption is widely adopted across sectors, the finance sector exhibits the highest adoption rate, emphasizing its critical role in protecting confidential information. On the other hand, the widespread use of MFA, particularly among senior-level employees, underscores its importance in access control. However, the discrepancies in adoption rates across sectors highlight the need for tailored security strategies to address sector-specific vulnerabilities and regulatory requirements.

A detailed examination of encryption algorithms, such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), can provide insights into the cryptographic techniques employed to secure data. Understanding the strengths and weaknesses of these algorithms is crucial for designing robust encryption systems that withstand modern cyber threats. Secondly, exploring the implementation of Multi-Factor Authentication (MFA) systems involves analyzing the engineering behind authentication protocols like OAuth, SAML, or biometric authentication methods.

Evaluating the efficiency and usability of these systems can inform the design of user-friendly yet secure access control mechanisms. Additionally, delving into the technologies utilized in security audits, such as vulnerability scanners, intrusion detection systems (IDS), and log analysis tools, offers insights into the automated processes and algorithms used to identify and mitigate security risks. Furthermore, addressing the engineering challenges in balancing technological advancements with security requirements involves considering factors like

usability, scalability, and interoperability. Engineers must develop innovative solutions that not only leverage cutting-edge technologies but also prioritize security without compromising functionality or user experience. By integrating engineering perspectives into the discussion, a holistic understanding of the technological underpinnings of information security practices emerges, enabling the development of effective and resilient security solutions in rapidly evolving digital landscapes.

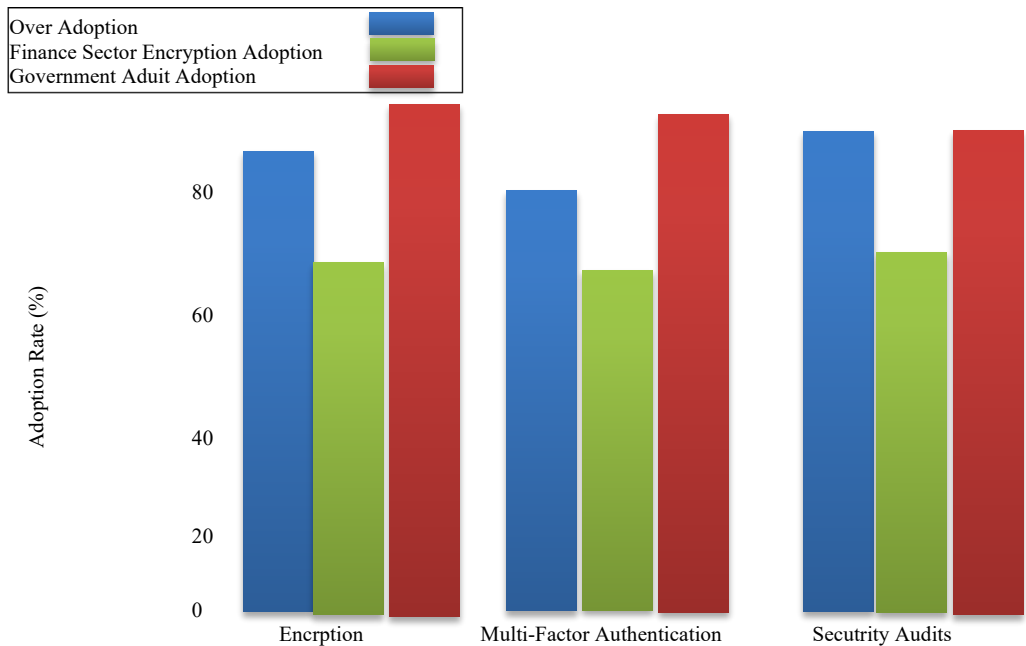


Figure 5. Adoption of information security measures [13]

Many organizations provide regular training on information security, but junior-level employees have shown lower awareness levels, indicating a need to improve training for all levels of employees. A significant number of organizations have a documented incident response plan, with a higher incidence in the healthcare sector. This shows the importance of having such plans as good practice. Security Information and Event Management (SIEM) Systems are used by a majority of surveyed organizations, especially in larger organizations where resource availability is better.

This highlights the need for SMEs to adopt such systems for enhanced cybersecurity resilience. Regular software updates and patch management are prioritized by most organizations, particularly in the finance sector, showing a proactive approach to addressing vulnerabilities. Finally, blockchain technology is used by a quarter of organizations for enhanced security, with a higher inclination in the technology and finance sectors, demonstrating blockchain's promise in specific industries. For more information about the statistical analysis of the legal question, please refer to Appendix B.

• **Takeaways from the Analysis:** The analysis shows that various information security measures are being adopted with a positive trend, but there are sector-specific

differences due to regulatory environments and industry-specific risk considerations. To further improve information security measures, it is recommended to run targeted awareness campaigns, knowledge-sharing initiatives, and sector-specific best practice forums. These findings highlight the importance of continuously adapting and being responsive to information security practices, to meet the changing challenges and take advantage of the opportunities in the dynamic digital landscape. This holistic approach can significantly contribute to strengthening the overall cybersecurity posture across various sectors.

6.3. Legal Framework Analysis

The findings reveal some key insights. Firstly, the level of awareness about legal obligations in this domain is moderate, indicating a significant knowledge gap among professionals, particularly those in small and medium-sized enterprises. Although the UAE's legal frameworks are generally viewed positively, a notable minority perceives room for improvement, indicating the need for more streamlined and stable legal frameworks.

Compliance challenges, including the complexity of laws and rapid regulatory changes, highlight the necessity for more accessible and stable legal frameworks. Many

organizations report inadequate legal support and resources, pointing to a resource gap in legal expertise. Recent legal changes are mostly viewed positively, but some participants feel adversely affected, suggesting the need for more inclusive and considerate legal reforms. The data indicates a deficiency in regular legal training and updates, emphasizing the need for ongoing education and awareness programs. Additionally, there is a general perception that legal frameworks are not fully keeping pace with technological advancements, necessitating more dynamic legal responses. Suggestions for legal improvement include clearer regulations, timely updates, and better support for compliance, underlining a need for more agile and transparent legal processes.

The findings highlight some important takeaways and lessons that can help improve legal awareness and compliance. These include the need to enhance legal education, simplify legal compliance, allocate more resources for legal support, ensure a balance between legal reforms and technological advancements, incorporate diverse stakeholder input for inclusive legal reforms, and develop agile legal frameworks that can adapt quickly to new challenges and technological developments. Addressing these challenges and opportunities can create a more secure digital environment, with a well-informed and legally compliant professional community in the UAE. This analysis provides valuable insights into the current state of legal awareness and compliance related to intellectual property and information security. It also points towards critical areas for policy development and organizational focus in the rapidly evolving digital landscape of the UAE. For more information about the statistical analysis of the legal question, please refer to Appendix C.

Figure 1, illustrates trends in legal awareness levels among various industry sectors over time, we can identify sector-specific challenges and opportunities. By closely scrutinizing the depicted trends, we can discern any significant shifts or patterns in legal awareness levels across different sectors. This analysis enables us to understand the dynamics of legal awareness within each industry and identify areas where targeted legal education and compliance initiatives are most needed. For example, sectors experiencing a decline in legal awareness may require focused efforts to enhance education and training programs, while those exhibiting upward trends may benefit from reinforcement and expansion of existing initiatives.

Table 2 provides valuable insights into the effectiveness of different compliance strategies, including training programs, technology investments, and regulatory audits. By assessing the outcomes of these strategies, organizations can gauge their relative efficacy in achieving legal compliance and mitigating associated risks. For instance, a comparison of the effectiveness of training programs versus technology investments may reveal which approach yields better results in enhancing compliance levels. This analysis informs decision-making processes regarding resource allocation and strategy

development, enabling organizations to optimize their compliance efforts based on empirical evidence.

A comparison of the results and simulation outputs related to different compliance methods allows us to evaluate their respective effectiveness. For instance, we can assess the advantages and disadvantages of regulatory audits versus employee training programs in enhancing legal compliance. By conducting this comparative analysis, organizations can gain valuable insights into the strengths and limitations of each approach, enabling them to make informed decisions about compliance management strategies. This information is crucial for designing tailored initiatives that align with organizational objectives and resource constraints.

In exploring engineering solutions for legal compliance, such as automated compliance monitoring systems and blockchain technology for secure record-keeping, we can identify opportunities for streamlining compliance processes and enhancing overall effectiveness. By leveraging technology, organizations can improve efficiency, accuracy, and transparency in compliance management. However, it is essential to consider potential challenges, such as implementation costs and data security concerns, associated with these solutions. Through thoughtful consideration and strategic planning, organizations can harness the power of engineering solutions to strengthen their legal compliance frameworks and ensure adherence to regulatory requirements. By delving into these specific aspects of the legal framework analysis, stakeholders can gain deeper insights into legal compliance trends and strategies. Moreover, this detailed examination enables organizations to make informed decisions and implement targeted initiatives to ensure compliance with legal obligations effectively.

- **Suggestions for Legal Improvement:** Suggestions for clearer regulations, more frequent updates in line with technological changes, and increased support for businesses in compliance were made.

6.4. Open-Ended Questions Analysis (Survey and Interviews)

Analyzed the interview questions. Legal analysis first, followed by general analysis to address challenges, opportunities, and insights.

6.5. Legal Analysis

- **Alignment with International Standards:** Most respondents feel that the UAE's legal frameworks are somewhat aligned with international standards, but there's room for improvement, especially in terms of rapid adaptability to global cybersecurity trends.
- **Legal Challenges in Cybersecurity:** A common challenge for organizations is keeping up with evolving cybersecurity laws and complying with them. The pace at which legal adjustments are required, particularly in response to new cybersecurity threats, is a struggle for many.
- **Effectiveness of Intellectual Property Enforcement:** Respondents have mixed opinions on the effectiveness of enforcing intellectual property rights. While some

acknowledge recent improvements, others highlight gaps, especially in digital spaces and e-commerce platforms.

- **Legal Support and Resources:** A significant number of organizations report lacking adequate legal support and resources. SMEs in particular find it difficult to keep up with complex legal requirements.
- **Impact of Emerging Technologies:** Emerging technologies present both opportunities and challenges for protecting intellectual property, as they bring new legal complexities. Discussions and concerns around the legal implications of AI and blockchain technologies are ongoing.
- **Regulatory Compliance and Business Operations:** Compliance with legal frameworks is often viewed as burdensome and resource-intensive, especially in sectors like finance and healthcare, where regulations are stringent.
- **Legal Preparedness for Data Breaches:** Many organizations lack confidence in their legal preparedness for data breaches, especially those handling sensitive data.
- **Recommendations for Legal Policy Makers:** Suggestions for policymakers: simplify legal processes, provide guidance for SMEs, and foster collaboration between legal community and technologists.
- **Awareness and Training on Legal Aspects:** Improved training and awareness programs on legal aspects are necessary. Organizations need to educate their employees more about cybersecurity and intellectual property laws.
- **Legal Trends and Future Outlook:** As digital transformation accelerates; respondents anticipate the need for more stringent laws and the evolution of legal frameworks to keep pace with technological advancements.

6.5.1. Analysis Takeaways

Based on the responses received, it appears that the legal frameworks for intellectual property and information security in the UAE are gradually improving. However, there is a growing need for more clarity, support, and flexibility especially for small and medium-sized enterprises (SMEs). Organizations are looking for simpler legal guidelines that are easy to understand, align with global standards, and can quickly adapt to technological advancements. The findings suggest that there is a clear need for better legal training and awareness, and policymakers should engage more closely with businesses to better understand their challenges. Overall, the results indicate that there is a transition in the legal landscape, providing ample opportunities for improving legal preparedness, compliance support, and enforcement effectiveness.

6.6. Challenges

6.6.1. Lack of Awareness

- Several respondents highlighted a prevailing lack of awareness regarding the importance of intellectual property rights and information security. This was particularly noted among small and medium-sized enterprises (SMEs). "Small businesses often

underestimate the value of their intellectual property, and there's a general lack of awareness about the potential risks associated with inadequate information security."

6.6.2. Compliance Burden

- Participants from regulated industries expressed concerns about the complexity and burden of complying with existing legal frameworks. Some mentioned challenges in aligning internal practices with rapidly evolving legal requirements. "Keeping up with the ever-changing legal landscape is a significant challenge. Compliance feels like a moving target, and it's resource-intensive."

6.6.3. Human Factor

- A common theme emerged regarding the human factor as a potential weak link in information security. Respondents cited the need for comprehensive employee training to mitigate the risk of unintentional breaches. "No matter how advanced our technologies are, the human element remains a significant challenge. We need more emphasis on continuous training to foster a security-conscious culture."

6.7. Opportunities

6.7.1. Technology Integration

- Respondents expressed optimism about the potential for emerging technologies to enhance information security. Blockchain, in particular, was highlighted for its potential to provide secure and transparent solutions. "Blockchain technology presents exciting opportunities for secure data storage and transparent transactions. Exploring these innovations could significantly strengthen our information security".

6.7.2. Collaboration and Knowledge Sharing

- Opportunities for collaboration and knowledge sharing between public and private sectors were emphasized. Participants saw potential in collective efforts to address common challenges. "There's room for more collaboration between government and private entities. Sharing best practices and insights could elevate the overall security posture in the UAE".

6.7.3. Investment in Education

- Several respondents suggested increased investment in educational programs to raise awareness about intellectual property rights and the importance of robust information security practices. "Education is key. We should invest in programs that not only raise awareness among businesses but also empower individuals to contribute to a secure digital environment".

6.8. Additional Insights

6.8.1. Call for Regulatory Clarity

- A notable comment was a call for clearer and more standardized regulations. Respondents expressed the need for well-defined guidelines to navigate the legal landscape effectively.

"Regulatory clarity is essential. Ambiguities in the law can lead to inadvertent violations. Clear and concise regulations would be tremendously helpful."

6.8.2. Balancing Innovation and Security

- Some participants highlighted the delicate balance between fostering innovation and maintaining robust security measures. Striking this balance emerged as a key consideration for organizations in the UAE. "We need to find a middle ground where innovation thrives, but not at the expense of compromising our security. It's a delicate balance that requires thoughtful consideration".

The analysis suggests that there has been a positive trend in the adoption of various information security measures across different sectors. However, there are some variations that highlight how sector-specific priorities and regulatory environments can influence the adoption of these measures. To enhance information security measures across the board, the study recommends targeted awareness campaigns and knowledge-sharing initiatives. The findings also point towards the need for an integrated approach to policy-making that takes into account the dynamic interplay between technology, legal frameworks, and information security.

In conclusion, the study's findings emphasize the intricate relationship between intellectual property, technology, and information security in the UAE. Therefore, a collaborative effort is necessary among government entities, private organizations, and legal bodies to ensure a secure and innovative digital environment. This environment should thoughtfully maintain the delicate balance between technological advancement and security.

7. CONCLUSION

This study looks at the connection between information security, technology, and intellectual property rights in the United Arab Emirates. It has been shown that, particularly among small and medium-sized businesses, there is a dearth of knowledge on intellectual property rights. This emphasizes the necessity of focused awareness campaigns to increase understanding and give intellectual property top priority in security plans. The respondents had a favorable opinion of using technology to secure information. Encryption and emerging technologies like blockchain were seen as promising ways to safeguard intellectual property. However, they also identified concerns about the human factor, particularly in terms of training and awareness. Challenges cited included a lack of awareness, compliance burdens, and the human factor, indicating a need for a nuanced approach to address industry-specific needs and create a security-conscious culture. Overall, participants expressed optimism about the potential of emerging technologies, collaboration, and increased education to address these challenges. They recommended targeted educational programs, regulatory clarity, and fostering collaboration between government and private sectors.

The study's conclusions have important ramifications for practitioners and policymakers. It draws attention to the

necessity of education and awareness campaigns to close the knowledge gap that exists between people and corporations. To solve this issue, policymakers are urged to make investments in increasing awareness. The study also emphasizes the importance of regulatory clarity. Policymakers should work towards creating transparent and standardized regulations to guide organizations in their information security and intellectual property protection efforts. Moreover, exploring opportunities for collaboration between government and private entities can lead to shared insights and best practices, which can improve the overall security strength in the UAE.

As the UAE continues its path of technological advancement, it is crucial to strike a balance between promoting innovation and maintaining strong security measures. Achieving this balance requires collaborative efforts from stakeholders across different industries. Although the study provides valuable insights, it acknowledges some limitations, such as the sample size. Therefore, future research should delve deeper into industry-specific challenges and opportunities to refine information security and intellectual property protection strategies. In conclusion, our study highlights the intricate relationship between intellectual property, technology, and information security in the UAE. It emphasizes that by addressing the identified challenges and capitalizing on opportunities, stakeholders can contribute to a resilient and secure digital environment. This will ensure the protection of intellectual capital for generations to come.

ACKNOWLEDGMENT

The authors express gratitude to the study's respondents for their participation, contributing to the success of this work.

REFERENCES

- [1] K. Aboelazm, "The Role of Digital Transformation in Improving the Judicial System in the Egyptian Council of State: An Applied Study from a Comparative Perspective", *Journal of Law and Emerging Technologies*, Vol. 2, No. 1, pp. 11-50, 2022.
- [2] K.S. Aboelazm, "The Debatable Issues in the Rule of Law in British Constitutional History and the Influence in the Egyptian Constitutions", *International Journal of Doctrine, Judiciary and Legislation*, Vol. 4, No. 2, pp. 521-568, 2023.
- [3] S. Aboelazm, "The Constitutional Framework for Public Policy in the Middle East and North Africa Countries", *International Journal of Public Law and Policy*, Vol. 7, No. 3, PP.187-203, 2021.
- [4] K. Aboelazm, "E-Procurement in the International Experience: An Approach to Reduce Corruption in Administrative Contracts in Egypt", *International Journal of Procurement Management*, Vol. 15, No. 3, pp. 340-364, 2021.
- [5] K.S. Aboelazm, "Policies and Legal Framework of Involving Small and Medium Enterprises in Administrative Contracts in Egypt: Dynamics and Influences", *International Journal of Public Law and Policy*, Vol. 9, No. 1, pp. 61-74, 2023.

- [6] K.S. Aboelazm, "The Development of the President's Authorities I.N the Egyptian Constitutions", Russian Law Journal, Vol. 11, No. 2, pp. 34-38, 2023.
- [7] K.S. Aboelazm, "The Legal Framework and Policies for Sustainable Administrative Contracts in Egypt: Reality and Challenges", International Journal of Public Law and Policy, Vol. 9, No. 2, pp. 111-129, 2023.
- [8] K. Aboelazm, "The Role of Judicial Review on the Acts of Sovereignty in Egypt", CEMJP, No. 31, Vol. 1, pp. 485-495, 2023.
- [9] S. Aboelazm, "The Success of the E-voting to Enhance the Political Engagement: A Comparative Study", Journal of Law and Sustainable Development, Vol. 11, No. 11, pp. 17-32, 2023.
- [10] K.S. Aboelazm, "Using E-Tenders in the United Arab Emirates to Enhance Transparency and Integrity", Kurdish Studies, Vol. 12, No. 1, pp. 91-102, 2024.
- [11] K.S. Aboelazm, S.A. Ramadan, "Transformation to E-Public Procurement in the United Arab Emirates in the Light of Uncitral Model Law", Journal of Law and Sustainable Development, Vol. 11, No. 8, p. e1499, 2023.
- [12] E.F.G. Ajayi, "Challenges to Enforcement of Cyber-Crimes Laws and Policy", Journal of Internet and Information Systems, Vol. 6, No. 1, pp. 65-69, 2016.
- [13] N. Kardani, A. Bardhan, S. Gupta, P. Samui, "Predicting Permeability of Tight Carbonates Using a Hybrid Machine Learning Approach of Modified Equilibrium Optimizer and Extreme Learning Machine", Acta Geotechnica, Vol. 1, No. 2, pp. 12-17, 2021.
- [14] H. Al Khalifah, P. Glover, P. Lorinczi, "Permeability Prediction and Diagenesis in Tight Carbonates Using Machine Learning Techniques", Mar Petrol Geol Vol. 1, No. 2, pp. 1102-14096, 2020.
- [15] S. Al Sharieh, "The Intellectual Property Road to the knowledge economy: Remarks on the Readiness of the UAE Copyright Act to Drive AI Innovation", Law, Innovation and Technology, Vol. 13, No. 1, pp. 34-35, 2021.
- [16] E. Andrijcic, B. Horowitz, "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property", In Risk Analysis, Vol. 26, No. 4, pp. 545-456, 2006.
- [17] J. Arato, "The Private Law Critique of International Investment Law", American Journal of International Law, Vol. 113, No. 1, pp. 12-15, 2019.
- [18] J.A. Brander, V. Cui, L. Vertinsky, "Intellectual Property Rights: A Challenge to the Rule of Law", Journal of International Business Studies, Vol. 48, No. 7, pp. 45-47, 2017.
- [19] C.J. Canby, "Pushing the Boundaries: Extraterritoriality, Patent Infringement Damages, and the Semiconductor Industry", Texas Law Review, pp. 10-14, 2023.
- [20] J.A. Casaca, T. Florentino, "Information Security Research: Actual Trends and Directions", Conference of Informatics and Management Sciences Vol. 8, pp. 251-256, 2014.
- [21] U. Cemalovic, "Intellectual Property Rights and Digital Transformation in Estonia-Aspects Related to Copyright and Patent Protection", Foreign Legal Life, Vol. 65, No. 4, pp. 701-713, 2021.
- [22] A.H.D Silva, S. Habermann, C.L. Craven, D.P. O'Hare, M. Jorgensen, K. Aquilina, "Atypical Teratoid Rhabdoid Tumours (Atrts) A 21-Year Institutional Experience", Childs Nervous System, Vol. 39, No. 6, pp. 1509-1518, 2023.
- [23] M. Charitonidou, "Urban Scale Digital Twins in Data Driven Society: Challenging Digital Universalism in Urban Planning Decision-Making", International Journal of Architectural Computing, Vol. 20, No. 2, pp. 238-253, 2022.
- [24] A. Ekramifard, H. Amintoosi, A.H. Seno, A. Dehghantanha, R.M Parizi, "A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence", Blockchain Cybersecurity, Trust and Privacy, Vol. 1, No. 2, pp. 147-160, 2020.
- [25] C. Fink, K.E. Maskus, Y. Qian, "The Economic Effects of Counterfeiting and Piracy: A Review and Implications for Developing Countries", World Bank Research Observer, Vol. 31, No. 1, pp. 23-36, 2016.
- [26] E. Sala, E. Martiri, "ADR Project Planning TO Increase Cyber Security Awareness of Mobile Device Users", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 56, Vol. 15, No. 3, pp. 327-333, September 2023.
- [27] H.M.H. Al Araj, A.I.H. Al Zughaibi, E.Q. Hussein, "Testing Two Types OF Magneto-Rheological (Mr) Damper Models with Quarter Car Suspension System Response", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 52-61, March 2023.
- [28] S. Javed, A. Tripathy, "An Approach Towards Demand Response Optimization at the Edge in Smart Energy Systems Using Local Clouds", Smart Energy, Vol. 1, No. 2, pp. 100-123, 2023.
- [29] S. Javed, J. Van, H. Mokayed, J.A Delsing, "Smart Manufacturing Ecosystem for Industry 5.0 Using Cloud-Based Collaborative Learning at the Edge", NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Vol. 1, No. 2, pp. 1-6, 2023.
- [30] H.Y. Khudhair, A. Mardani, "The Major Issues Facing Staff in Islamic Banking Industry", International Journal of Economics and Management Systems, Vol. 3, No. 6, pp. 45-48, 2021.

BIOGRAPHIES



Name: Mohammad

Middle Name: Njim

Surname: Elyat

Birthday: 22.01.1986

Birthplace: Jordan, Jerash

Bachelor: Law, Faculty of Law, Yarmouk University, Irbid, Jordan, 2009

Master: Law, Department of Public Law, Faculty of Law, University of Jordan, Amman, Jordan, 2011

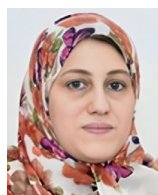
Doctorate: Public Law, Faculty of Law, Department of Public Law, University of Jordan, Amman, Jordan, 2015

The Last Scientific Position: Assist.t Prof., Department of

Public Law, Faculty of Law, Arab Open University, Muscat, Oman, 2023

Research Interests: Administrative Law, General Functional, and Administrative Organization

Scientific Publications: 2 Papers



Name: **Nadia**

Middle Name: **Yas**

Surname: **Al Bayati**

Birthday: 05.05.1978

Birthplace: Iraq, Baghdad

Bachelor: Law, Faculty of Law, Misrata University, Misurata, Libya, 2003

Master: Civil Law, Faculty of Law, University of Juba, Juba, Sudan, 2009

Doctorate: Civil Law, Faculty of Law, International Islamic University, Kuala Lumpur, Selangor, Malaysia, 2013

The Last Academic Position: Assist. Prof., College of Law, Al Falah University, Dubai, UAE, 2017-2022

Research Interests: Civil Law, Contracts, Insurance Contracts, Liability for Harmful Actions, Civil Liability, Electronic Transactions, Artificial Intelligence Issues.

Scientific Publications: 8 Papers



Name: **Nuha**

Middle Name: **Anwar**

Surname: **Al Baloushi**

Birthday: 01.07.1985

Birthplace: Al Ain, UAE

Bachelor: Applied Science in Business Administration, Al Ain Women's

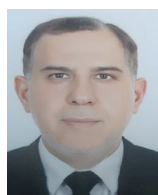
College, Al Ain, Abu Dhabi, UAE, 2014

Master: Leadership and Organizational Development, Abu Dubai School of Management, Abu Dubai, UAE, 2019

Doctorate: Student, Business Management, British University of Dubai, Dubai, UAE, Since 2020

Research Interests: Artificial Intelligence in Management, Blockchain Technology in Industrial Processes

Scientific Publications: 7 Papers



Name: **Mohammed**

Middle Name: **Ibrahim**

Surname: **Sarhan**

Birthday: 03.03.1970

Birthplace: Basra, Iraq

Bachelor: Sharia, Faculty of Sharia, Yarmouk University, Irbid, Jordan, 2001

Master: Sharia and Law, Faculty of Sharia and Law, Al-Zaim Al-Azhari University, Khartoum, Sudan, 2009

Doctorate: Sharia and Law, Faculty of Sharia and Law, Holy Quran University of Islamic Sciences, Omdurman, Sudan, 2012

The Last Academic Position: Assist. Prof., College of Law, Umm Al Quwain University, Umm Al Quwain, Kabir, UAE, Since 2022

Research Interests: Comparative Law, Comparative Jurisprudence

Scientific Publications: 5 Papers



Name: **Adam**

Middle Name: **A.**

Surname: **Marks**

Birthday: 01.04.1986

Birthplace: Dubai, UAE

Bachelor: Information System, Faculty of Information System, University of Central Florida, Florida, USA, 2007

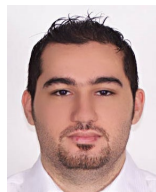
Master: Management of Information System, Faculty of Business, University of Central Florida, Florida, USA, 2014

Doctorate: Management, Faculty of Information System, University of Central Florida, Florida, USA, 2019

The Last Scientific Position: Academic, Lecturer, Department of Information System, University of Sharjah, Sharjah, UAE, 2023

Research Interests: Management, Innovation, Information System

Scientific Publications: 4 Papers



Name: **Harith**

Middle Name: **Yas**

Surname: **Khudhair**

Birthday: 19.10.1986

Birthplace: Dubai, UAE

Bachelor: Management, Faculty of Management, Ajman University,

Fujairah, UAE, 2008

Master: Technology Management, Faculty of Business, Staffordshire University, Kuala Lumpur, Malaysia, 2012

Doctorate: Management, Faculty of Management, Technological University of Malaysia, Johor Bahru, Malaysia, 2021

The Last Scientific Position: Academic Lecturer, Department of Management, Faculty of Business, Technological University of Malaysia, Kuala Lumpur, Malaysia, Since 2021

Research Interests: Manufacturing, Business Administration, Marketing, Management, Innovation, Quality Management, Customer Satisfaction, Service Quality

Scientific Publications: 30 Papers



Name: **Adel**

Middle Name: **Salem**

Surname: **Allouzi**

Birthday: 26.11.1975

Birthplace: Amman, Jordan

Bachelor: Law, Jordan University, Amman, Jordan, 1997

Master: Law, Jordan University, Amman, Jordan, 1999

Doctorate: Private Law, Amman Arab University, Amman, Jordan, 2004

The Last Scientific Position: Dean, Assoc. Prof., Law, Abu Dhabi University, Abu Dhabi, UAE, Since 2012

Research Interests: Private Law, Civil Law, Civil Procedure Law, Arbitration, Mediation

Scientific Publications: 15 Papers, 1 Book

Scientific Memberships: Jordanian Bar Association