**National University of Computer & Emerging Sciences**

**Karachi Campus**

****

**Information Security**

**Project Report**

**Group Member**

**21k-3840 Israr Ali**

**21k-3841 Ahmad Noor Khan**

**21k-3842 Naresh Kumar**

**21k-3881 Taha Jawaid**

**Evaluation of the accuracy of the neural network algorithm for object recognition in security systems**

**Summary:**

The document discusses the performance evaluation of neural network algorithms for object recognition, particularly in the context of security systems. It emphasizes the importance of various metrics to assess the quality and effectiveness of these algorithms. Key metrics include Intersection over Union (IoU), which measures the accuracy of predicted segmentations against ground truth, and other evaluation metrics that help in objectively assessing model performance.

The study utilizes the CamVid benchmark video dataset for training, revealing significant variability in recognition accuracy across different classes, ranging from 38.15% to 97.07% when using the VGG-16 function. The analysis indicates that the quality of training data—encompassing aspects like data quality, quantity, preprocessing, algorithm complexity, and the training process—plays a crucial role in the accuracy of image recognition.

The findings suggest that while some classes achieve high accuracy, others, such as "Pavement," exhibit lower performance, indicating a need for improved training data. The document concludes that enhancing the dataset and refining the training process are essential for boosting the overall effectiveness of neural network-based object recognition systems, particularly in applications like intelligent access control and machine vision systems.

**Analysis of identification and access management models in the context of fog computing**

**Summary:**

The document analyzes various identification and access management (IAM) models in the context of fog computing, which is characterized by a hierarchical structure involving cloud, fog, and edge layers. Fog computing enhances data processing efficiency by distributing tasks across multiple nodes, but it also introduces challenges in managing identification and access due to its decentralized nature.

The paper discusses several IAM models:

1. Single Sign-On (SSO): This model allows users to authenticate once and gain access to multiple systems without re-entering credentials. While it increases user convenience, it poses a security risk; if one account is compromised, all connected systems may be vulnerable.

2. Federated Identity Management (FIM): FIM enables a single user identification system across different organizations, allowing users to access resources without creating multiple accounts. This model centralizes access management but requires complex coordination and can be challenging to maintain.

3. Role-Based Access Control (RBAC): RBAC assigns access rights based on user roles within an organization, simplifying access management for large groups. However, it lacks flexibility, as roles must be manually updated to reflect changes in responsibilities.

4. Attribute-Based Access Control (ABAC): ABAC offers a more flexible approach by granting access based on various user attributes, such as location and time, allowing for fine-tuned access rights. This model is more complex but can adapt to dynamic environments.

5. Zero Trust Model (ZTM): ZTM operates on the principle of "never trust, always verify," requiring continuous authentication and validation of users and devices, regardless of their location within or outside the network. This model enhances security but can complicate access management.

The paper emphasizes that the dynamic nature of fog computing, with devices frequently connecting and disconnecting, complicates the implementation of uniform access policies. Many devices in fog environments rely on single-factor authentication, making them vulnerable to attacks. The authors argue that a robust IAM system is crucial for protecting sensitive data and ensuring secure access in fog computing, especially in critical infrastructure scenarios.

In conclusion, the document highlights the importance of selecting appropriate IAM models tailored to the unique challenges posed by fog computing. It advocates for a balanced approach that considers both security and usability to effectively manage access in increasingly complex and distributed environments.

**Simulation model of information system transformation to increase survivability against cyber threats**

**Summary:**

The document discusses the critical issue of enhancing the survivability of information systems in the face of increasing cyber threats and malicious influences. It emphasizes the need for a comprehensive approach to ensure the functionality of these systems during adverse conditions, particularly in the context of warfare and cyber-attacks. The authors, Yuriy Syvytsky and Viktor Shevchenko, highlight that survivability involves not only technical solutions but also the transformation of organizational and information structures.

The paper identifies a significant gap in existing research regarding practical methods for modeling and optimizing the structural transformation processes of information systems. To address this, the authors propose the development of dynamic simulation models that can forecast the consequences of management decisions and identify optimal solutions for structural transformations. This approach aims to increase the effectiveness of information structures in adapting to new projects and threats.

The authors also discuss the complex nature of information and cyber security management, which extends beyond technical aspects to include regulatory frameworks and standards, such as those set by NIST. They stress the importance of an objective assessment of security states and threats, necessitating specific methods for obtaining numerical estimates of information security levels. The paper references various studies that explore security metrics for distributed wireless systems and communication systems under cyber-attack conditions.

Furthermore, the authors present results from their modeling efforts, demonstrating significant improvements in the integral quality criterion of information security levels. They note that while the duration of critically low protection levels has decreased, the overall security level should not be deemed satisfactory, indicating ongoing challenges in achieving robust security.

In conclusion, the paper advocates for a systematic approach to enhancing the survivability of information systems through simulation modeling and structural transformation. By integrating theoretical and applied methodologies, the authors aim to provide a framework that can effectively respond to the evolving landscape of cyber threats, ultimately contributing to the resilience of information systems in various operational contexts.

**Cybernetic cognitive model for describing the financial health of it gaming company**

**Summary:**

The document presents a comprehensive study on the development of a cybernetic cognitive model aimed at analyzing the financial condition and performance indicators of IT gaming companies. The primary objective is to enhance the accuracy of predictions regarding financial outcomes by considering various influencing factors. The authors propose a software implementation of this cognitive model using Python, leveraging libraries such as NetworkX and Matplotlib for visualization and data analysis.

The cognitive model is structured as a directed graph, where nodes represent financial performance indicators and external factors, while edges illustrate the cause-and-effect relationships between these concepts. This graphical representation allows for a clear visualization of how different variables interact, enabling management to make informed decisions based on the analysis of these relationships.

Key components of the proposed software architecture include a cognitive modeling module for graph visualization and simulation, a data module for integrating external data sources, and a reporting module for generating insights based on the analysis. The system is designed to be flexible and adaptable, allowing for the addition of new modules tailored to specific company needs, such as risk management or supply chain analysis.

The document emphasizes the importance of data security and confidentiality, particularly in the context of the ongoing military aggression in Ukraine, which has heightened the need for stringent security measures in financial data management. The authors highlight that different companies may have varying requirements for data protection, depending on their industry and operational context.

Furthermore, the research underscores the significance of early diagnosis of financial issues through the use of cognitive modeling. By identifying potential financial instability early on, companies can take timely corrective actions to mitigate risks and prevent bankruptcy. The integration of cognitive models into decision support systems (DSS) is presented as a means to facilitate real-time monitoring of financial performance, allowing for the identification of deviations and threats.

In conclusion, the study advocates for the adoption of cognitive modeling in financial management, particularly for IT gaming companies operating in a rapidly changing environment. The proposed model not only aids in forecasting financial performance but also enhances the overall decision-making process by providing a robust analytical framework. The findings suggest that such systems can significantly improve financial planning, optimize costs, and ultimately enhance the performance of businesses in the gaming industry.

**Distribute load among concurrent servers**

**Summary:**

The document discusses a proposed technique for load balancing in application servers, emphasizing the need for stability in request distribution amidst unpredictable fluctuations. The core of the strategy involves a software server that autonomously manages multiple application servers, facilitating real-time adaptive distribution of requests to achieve uniform load balancing. This approach is grounded in a theoretical framework that addresses the dynamics of incoming request flows, which are characterized as random and non-stationary.

The paper introduces a structural and functional model designed to operate under conditions of varying request intensity. It outlines a mechanism for redistributing incoming requests from overloaded servers to those with lighter loads, thereby ensuring a more balanced server load. The model incorporates various functional components, including a request queue buffer, a smoothing step generator, and a demultiplexer for managing request streams.

Additionally, the document critiques traditional traffic management methods, such as the "token bucket" approach, suggesting that they may not be suitable for adaptive load redistribution in non-stationary environments. Instead, it proposes enhancements to these methods to better accommodate the characteristics of actual traffic flows.

Overall, the paper highlights the importance of developing dynamic load balancing mechanisms to prevent server overloads and maintain efficient application system performance in the face of fluctuating request patterns.

**The system of secured user’s credentials transfer**

**Summary:**

The document presents a comprehensive approach to enhancing the security of user authentication in web applications through a 10-level encryption algorithm designed for the secure transmission of user credentials, specifically login and password data. The algorithm aims to mitigate risks associated with common cyber threats, such as Man-in-the-Middle (MITM) and Brute force attacks, which can lead to unauthorized access and data breaches.

The process begins with the user submitting their encrypted login and password to the web application server. The server then employs a hashing function to compare the received credentials with those stored in the database, generating a one-time token (Salt) for added security. This step is crucial as it ensures that the data is not directly exposed to potential SQL injection attacks. The algorithm includes multiple verification levels, each executing specific procedures to validate the input data and prevent malicious code from being processed.

Upon successful verification of the credentials, a final one-time access token is generated, granting the user access to the web application’s internal resources. This token is also stored in the database, ensuring that it cannot be reused, which further protects against MITM attacks. The system is designed to log failed login attempts, blocking user accounts and IP addresses after a set number of unsuccessful attempts, thereby preventing Brute force attacks.

The paper emphasizes the importance of this algorithm for small and medium-sized businesses (SMBs) and startups, which may not have the resources to invest in commercial security solutions. By implementing this 10-level algorithm, these companies can effectively safeguard user credentials and personal data during the initial stages of their development, reducing the risk of data leaks and cyber threats.

In conclusion, the proposed high-level design system not only provides a detailed framework for secure data transmission but also serves as a practical solution for businesses looking to enhance their cybersecurity measures without relying on third-party technologies. The algorithm's structured approach to user authentication and data protection represents a significant advancement in the field of web application security.

**Method of speech signal scrambling based on matched wavelet filters**

**Summary:**

The research paper presents a novel method for protecting speech information through the use of digital wavelet filter banks, specifically employing matched wavelet filters (MWFs). The primary objective of this study is to develop a reliable system that ensures the confidentiality of speech signals while allowing for their full recovery at the receiving end. The proposed algorithm is designed to operate in real-time, making it suitable for telecommunication environments where speech quality is paramount.

The paper discusses the evaluation of speech quality using two main metrics: PESQ (Perceptual Evaluation of Speech Quality) and an expert evaluation score denoted as Q. PESQ is a standardized method that compares the original and reconstructed signals, providing a score on a scale from 1 (poor) to 5 (excellent). A PESQ score greater than 2.5 indicates acceptable quality, while the Q score, which also follows a 5-point scale, suggests that a score greater than 3 corresponds to intelligible speech. The study emphasizes that the protection system must ensure that the transmitted signal is unintelligible while maintaining high intelligibility for the recovered signal.

The algorithm developed in this research utilizes MWFs during the analysis-synthesis filter bank construction, allowing for effective encryption of speech signals. The system is robust against noise and can function effectively in channels with significant interference, provided the noise level is above 25 db. The operating parameters of the protection system are derived from PESQ and Q estimations, ensuring a high degree of information closure and acceptable quality of the recovered signal. The study finds that the parameter settings for FIR and IIR filters yield different results, with FIR filters exhibiting lower quality due to error amplification.

The paper also explores the implications of quantization levels on the encrypted signal, revealing that 8 and 16-bit quantization are sufficient for secure transmission without necessitating higher levels. The authors highlight the importance of the orthogonality properties of MWFs, which facilitate the separation of the useful signal from the noise-like mixture created during transmission.

In conclusion, the research demonstrates the effectiveness of the proposed speech protection system, which combines advanced digital signal processing techniques with robust encryption methods. The findings indicate that the system can reliably protect speech information while ensuring high-quality recovery, making it a valuable contribution to the field of telecommunications and information security. The study also suggests that further exploration into key distribution methods and the optimization of filter parameters could enhance the system's performance and security

**Hardcoded credentials in Android apps: Service exposure and category-based vulnerability analysis**

**Summary:**

The paper titled "Hardcoded credentials in Android apps: Service exposure and category-based vulnerability analysis" by Olha Mykhaylova, Taras Fedynyshyn, and Artem Platonenko presents a comprehensive study on the security vulnerabilities associated with hardcoded sensitive credentials in Android applications. The research highlights the critical risks posed by the practice of embedding sensitive information, such as API keys and authentication tokens, directly within the application code.

The study involved the static analysis of 6,165 APK files downloaded from the Google Play Store, utilizing the Mobile Security Framework (MobSF) for initial assessments. This framework allowed the researchers to identify potential security vulnerabilities and insecure coding practices within the applications. Following this, the "secrets" section of each APK was scrutinized using Trufflehog, a tool designed to detect hardcoded secrets, to validate the presence of sensitive credentials and differentiate genuine secrets from false positives.

The findings revealed a concerning prevalence of hardcoded credentials across various applications, with many embedding sensitive information related to cloud service providers, payment gateways, and third-party APIs. The analysis categorized the occurrence of these vulnerabilities by app type, demonstrating that certain categories of applications exhibited higher rates of exposed credentials than others. This underscores the need for improved security practices in mobile app development, particularly regarding the secure management of sensitive information.

The paper emphasizes that despite the vetting processes employed by platforms like Google Play and Apple App Store, many applications still harbor significant vulnerabilities. The authors argue that the rapid evolution of mobile applications, coupled with the increasing responsibilities they bear, necessitates the development of more robust security methods and tools. They also highlight the inadequacy of existing security measures in addressing the growing number of mobile applications and the associated risks.

In conclusion, the study serves as a call to action for mobile app developers to adopt stronger security practices to mitigate the risks associated with hardcoded credentials. By identifying and analyzing these vulnerabilities, the research aims to provide valuable insights into improving the management of sensitive data within Android applications, ultimately enhancing the overall security of the mobile ecosystem.