International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

An In-Depth Analysis of & Performance Comparison Security Models Used In Banking Scenario

Suraj Pawar, Prof. Abhimanyu Dhutonde

Department of Computer Science and Engineering, Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 01 Sep 2023

Published: 08 Sep 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

10-29

ABSTRACT

The demands of the contemporary banking environment call for a sharp focus on security paradigms that protect the integrity and confidentiality of private financial information. The exposure to several cyber dangers increases as digitization quickens and transactions cross traditional boundaries. This study conducts a thorough examination of security models within the context of banking situations in response to this urgent requirement, attempting to shed light on their intricacies and efficacies through a discriminating comparative analysis. The complexity of cyber threats, which is increasing, necessitates security frameworks that go beyond conventional safeguards, which forms the basis of this work. In order to prevent breaches, safeguard customer data, and guarantee smooth operations, banking institutions must carefully consider and select the best security models. This paper examines the complexities of security models while closely examining their applicability and performance metrics in light of these imperatives. The review procedure used here combines in-depth literature analysis with empirical evaluation. The initial stage entails a thorough analysis of the security paradigms currently in use in banking situations. The fabric of these models is made up of multifactor authentication methods, intrusion detection systems, access control mechanisms, and cryptographic techniques. This thorough evaluation lays the groundwork for the comparative study that follows, which depends on crucial parameters including precision, accuracy, complexity, deployment cost, and scalability levels. The report carefully examines the interplay of evaluative criteria and analyses the strengths and weaknesses of each security model. This approach concludes with a sharp evaluation that highlights the differences in their abilities to fend off cyberthreats and survive the rigours of the banking environment. The abstract ends by stating that our work proves not just the necessity of sophisticated security models but also gives stakeholders, decision-makers, and practitioners a useful tool for wise model selections.

Keywords: Security Models, Banking Scenarios, Comparative Analysis, Precision, Accuracy, Complexity, Deployment Cost, Scalability, Empirical Study, Paradigms

I. INTRODUCTION

Security is still a crucial issue in the world of modern banking, there is no doubt about that. The expansion of complex financial transactions and the rise in digitalization have highlighted the need for strong security paradigms that protect the availability, confidentiality, and integrity of sensitive data. The vulnerability to cyber threats and breaches increases as banking systems become more linked and dependent on digital channels. As a result, implementing advanced security models has become crucial to bolstering banking institutions' defences against a variety of developing threats.

This paper sets out on an in-depth exploration of security models with a focus on banking settings. By examining these models' practical application and performance within the intricate and dynamic context of the banking domain, it seeks to analyse and assess their effectiveness via a lens that goes beyond simple theoretical abstractions. The main goal is to give stakeholders, decision-makers, and practitioners a thorough awareness of the security frameworks available to them and their complex characteristics.

One must first recognise the complex network of activities that supports financial institutions in order to fully appreciate the significance of security models in the world of banking. The intersection of client information, transactional records, and proprietary data highlights the need for security paradigms that go beyond simple defences. Although necessary, traditional security measures frequently fall short of reducing the complex dangers that characterise modern cyber ecosystems.

This research is grounded in the development of insightful understandings that go beyond cursory assessments and probe the fundamental capabilities of security models. The justification stems from the requirement for security models that are as sophisticated as the increasingly sophisticated cyber threats. The research makes an actual inquiry, complete with meticulous analysis and comparison, in an effort to clarify the practical advantages and constraints of various security models.

The approach of the paper is based on a painstaking synthesis of thorough literature review and empirical analysis. The first stage comprises a thorough analysis of the security paradigms that are currently in use, including protocols for multifactor authentication, intrusion detection systems, access control methods, and cryptographic methodologies. Then, a comparison matrix is built, with the key parameters being precision, accuracy, complexity, deployment cost, and scalability. These metrics act as the analytical compass that directs the assessment of each model's capability.

The remainder of this work is divided into well planned sections to allow for an organic development of ideas. The extensive literature analysis in Section II results in a comprehensive understanding of the numerous security models used in the banking industry. The methodological foundations are explained in Section III, along with the selection criteria for the evaluations. Section IV summarises the empirical data and compares and contrasts the identified security models. The discussion is contained in Section V, where the intricacies of the properties of the models are examined in light of the empirical results. Section VI, the paper's concluding remarks, summarises the paper's overall implications and the prospective trajectory of security models within the dynamic environment of banking situations.

The thematic framework and methodological foundations of this paper's quest are established by the introduction. The following parts will delve deeper into the complex realm of security models as they negotiate the challenging landscape of contemporary banking, building a link between conceptual frameworks and practical applications.

II. Literature Review

An Iterative & wide variety of models are proposed by researchers for improving security of banking transactions. Research in [1], for instance, highlighted

the significance of maintaining in-person banking interactions. It's possible that service robots used in hybrid bank branches might boost productivity and save expenses. Know-Your-Customer (KYC) processes that are both efficient and impartial are necessities for hybrid banking. In order to facilitate cyber-physical banking with the use of robots, this research offers a deep learning-based automated interbank KYC system. To protect the customer's privacy, the collected visual data was de-identified and modeled utilizing a very sophisticated biometric architecture. Secure, distributed transmission and verification of biometric data was achieved via the use of both the blockchain network and the symmetric-asymmetric encryption-decryption module. It is also recommended that personal financial records be encrypted during transmission and storage using a high-capacity fragile watermarking technology based on the integer-to-integer discrete wavelet transform in combination with the Z6 and A6 lattice vector quantization. The recommended architecture for the automatic biometric collecting of handwritten bank checks from customers in accordance with COVID-19 pandemic safety standards was validated via testing on a Pepper humanoid robot. The suggested framework uses a watermark to inscribe the fingerprint and identity of bank clients on the associated bank papers. The research shows that the suggested security protection framework may add more biometric data to bank papers than comparable algorithms. Plus, the quality of the encrypted financial papers is 20% better than with other suggested methods. In addition, the banking industry's privacy standards may be met by the hierarchical visual information interchange and storage module that obscures people's identities in machine-collected films. For future in-person banking, the suggested framework may provide a rapid, efficient, and cost-effective inter-bank solution that satisfies security needs and banking rules.

Bitcoin transactions may now be made completely anonymous thanks to decentralized anonymous payment (DAP), which is explained in detail in [2]. It has been suggested that DAPs use anonymous monetary systems like Zerocash or Monero to increase their security and privacy. However, the great degree of privacy may lead to new legal difficulties since criminals may abuse the anonymity of transactions for things like money laundering. In this study, we provide a novel DAP system that makes it easier to follow and enforce rules and laws. The standards for anonymous payments are set by regulators who are first exposed to the system. Commitments and non-interactive zero-knowledge proofs for provable claims are then used to enforce the rules. Users may then provide evidence that their dealings are entirely above board. In the event that authorities uncover questionable transactions, they will have access to a monitoring equipment that will reveal the real names of the users. The performance assessment and formal security model prove that the suggested approach is very successful, and they show that it is possible to provide the necessary security characteristics.

Recently, Qiao et al. (2021) have been working to design an effective certificateless signature (CLS) method and build a transaction system for IoT-based mobile payments, which is discussed in [3]. Claiming immunity from Type I and Type II assaults, they provide CLS as proof. In this article, we show how to use an attack vector against their CLS method, proving that it is vulnerable to Type II assaults. We also provide an improved CLS plan to further fortify their infrastructure.

As was noted in [4]'s research, To assess whether an Android APK is a banking trojan, we build the $sf DBank$ system using a new dataset of Android banking trojans (ABTs), other Android malware, and goodware. We provide the novel idea of a Triadic Suspicion Graph (TSG), which includes three categories of nodes: goodware, financial trojans, and API packages. We build a novel feature space using two scores obtained from TSGs: suspicion scores (SUS) and suspicion rankings (SR), the latter of which generates a family of features that generalize PageRank. In spite of the fact that TSG features (based on SUS/SR scores)

alone offer very high predictive accuracy in predicting recent (2016-2017) ABTs, we show that combining TSG features with previously researched lightweight static and dynamic features in the literature yields the highest accuracy in distinguishing ABTs from goodware while maintaining the accuracy of previous feature combinations in distinguishing ABTs from other Android malware. For instance, $sf DBank$ has a 99.9% AUC accuracy rate and 0.3% false positive rate when assessing if an APK is a banking trojan. We have also alerted the Google Android Security Team to the fact that $sf 'DBank'$ has detected two unlabeled APKs from VirusTotal as ABTs. We outperformed 62 of VirusTotal's 63 antivirus systems in one case, and we were the first to spot the unlabeled APK in another. This indicates that $sf 'DBank' is able to identify innovative environmental things before other well-known providers do. We also show that our innovative TSG features have impressive defensive capabilities by showing that they can withstand an attack from an enemy that is familiar with 90% of our training set and employs the same TSG features as ourselves. This makes it hard for the opponent to infer $sf DBank$'s forecasts with respect to APKs. We also detail the features that set ABTs apart from both goodware and other forms of Android malware. Finally, we distinguish the key features that set ABTs apart from goodware and other malware by conducting a detailed, data-driven examination of five major recent ABT families: FakeToken, Svpeng, Asacub, BankBot, and Marcher.

Correspondent banking involves a large number of intermediaries working across various time zones, making it impossible for existing interbank payment systems to provide cost-effective cross-border transactions. This was highlighted in [5] studies. They also have to deal with lengthy transaction delays and a lack of clarity. The creation of an auditable currency on a permissioned blockchain, which grants network control to an authorized party, might solve these problems. In this work, we introduce a consortium blockchain that uses bitcoin as its transaction output while keeping costs to a minimum. Power-efficient proof of authority consensus is implemented on the blockchain with full rights for all participating states. Unlike with more conventional cryptocurrencies, self-managed authentication may be carried out on-chain using dynamic decentralized identifiers (DIDs) serving as transactional addresses. Only the appropriate DID issuers will have access to the identities of the individuals involved in a transaction. This approach safeguards user privacy, provides transparency, and guarantees auditability in P2P financial transactions. Multiple calculation and signature methods are available for users' convenience. When the Python code for the system was complete, the transaction mechanism was tested. This paper may help to bolster ongoing investigations into potential applications of blockchain technology for international payments.

Yeh showed in 2018 that a certificateless signature (CLS) technique without bilinear pairing may be used to provide a secure transaction system for mobile payments. Because public communication networks are notoriously unsafe, this was done to ensure that mobile payments could be made safely. However, we highlight that this CLS approach is vulnerable to public key replacement attacks, which would allow malevolent users to produce authentic forging signatures for every new communication. The higher transaction mechanism is not as secure as it claims to be because of vulnerabilities in the underlying CLS system. This article shows that Yeh's method cannot provide the intended degree of security by explaining how a forgery attack against the CLS scheme works. A concrete CLS scheme structure with improved security is presented as a further solution to the aforementioned problems with security. Using the Forking lemma in a random oracle model, we can prove that our technique is preferable even if the discrete logarithm issue cannot be solved. Finally, we offer a safe payment solution for Android-based mobile devices based on our enhanced CLS techniques.

As said in [7], Concerns about the industry's fast growth have been raised in light of the serious risk

presented by online payment fraud. Rule-based and machine learning-based methods are widely used in the fraud detection industry. The sliding time frame is a common and efficient solution to this issue since the major features of such fraudulent transactions are given progressively. By adjusting the temporal window through which one looks at the data, one may learn more about the features of the transactions that have been recorded. However, the adaptive design of sliding time window is difficult because transaction patterns in real-world application settings are sometimes too elusive to be captured. In reality, configuration updates and improvements almost always need human interaction. This will take quite some time. In this research, online payment fraud is identified using a combination of automatic sliding time frames and an adaptive learning approach. As a result, we're working to make windows more flexible and optimize their current settings. We created an intelligent window—a learning automated window, or LAW. Using the ever-changing fraudulent transaction patterns as input, learning automata calculate the optimal time window parameters and regularly and dynamically adjust them. Using a real-world dataset from an online payment service provided by a commercial bank, we assess the value of LAW in terms of detection effectiveness and resilience. To the best of our knowledge, this is the first attempt to create a fraud detection time period that can adapt to different conditions.

There has been a rise in the usage of mobile applications for making financial transactions, as reported by [8]. There is a lack of transport layer security in the existing literature on mobile commerce and payments, making it vulnerable to reverse engineering assaults. This means that the attackers will likely be able to successfully penetrate the MPA and steal a significant amount of money. To address these concerns, we provide a defense-in-depth approach to security design for Near Field Communication (NFC) mobile payment systems. Our multi-layered approach to security includes safeguards at the hardware, mobile app, and network layers. Applying BAN (Burrows, Abadi, and Needham) logic and the Scyther tool, we successfully verified a mobile payment protocol and suggested an NFC-based Secure Protocol for Mobile Transaction (NSPMT). We successfully tested our suggested protocol against many protocols, RAM scraping assaults, DoS, DDOS, and Phlashing attacks, and found that it effectively repelled all of them. Our suggested mobile payment system is immune to attacks like Heartbleed and ROBOT (Return of Bleichenbacher's Oracle Threat), which target mobile applications. Our suggested protocol greatly reduces energy consumption, has reduced communication and processing costs, and provides full security, as compared to prior efforts in the literature. Our protocol has been successfully implemented using the Kotlin programming language and Android Studio to encrypt and decrypt Customer Payment Data at MPAs and PPAs using the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Advanced Encryption Standard (AES) with GCM (Galois/Counter Mode) modes.

Research published in [9] indicates that SSTs are becoming more commonplace in a variety of settings, from vending machines and self-service banking to automated national border crossing checkpoints. There are major security issues about the incorporation of SSTs into essential infrastructure. In this research, we provide a security model for the family of SST system protocols in an effort to give formal proof that existing SST architectures are vulnerable to attack. Our company provides a wide variety of attack setups designed to hit SST infrastructures in particular. We then utilize this inventory to verify that the following three strategies for increasing SST system resilience in the face of compromise are viable options. The suggested changes include a bootstrapping service, the replacement of free-range APIs with multi-signature transaction tokens, and the transformation of networking interfaces in SSTs into direct connections between devices. Our firm offers Offline Self-Service Things (OSST) that can keep a distributed representation running without an active network

connection and show remarkable resistance to outside intrusion attempts. The AutoThing framework was created with the intention of making it easier to put open-source software tools (OSSTs) into practice. Two examples, VolgaPay (a payment system for vending machines) and VolgaGuard (an access control system), demonstrate the flexibility of the AutoThing framework. A comparison is made between the two platforms to demonstrate AutoThings' flexibility and scalability.

According to the study cited in footnote [10], the mobile payment system is expected to provide increased efficiency and convenience in terms of payment options. The safety of digital wallets and payment applications is far more precarious with mobile payments than with more conventional options. The purpose of this research is to examine a popular tokenized mobile payment mechanism in order to identify possible security flaws and give a corresponding off-site attack approach. Aside from people with evil intent, illegal merchants might also play a role in this situation. In addition, we advocate for the implementation of SALP, a trusted and safe payment protocol that factors in both time and location as pivotal determinants in verifying monetary exchanges. The Secure Anti-Low Probability (SALP) system's main goal is to efficiently prevent attacks from off-site by focusing on prospective bad guys like dishonest shopkeepers. Identity-based signature (IBS) is used to avoid relying on a third party to verify transactions and to safeguard data against manipulation. Case examples are presented that show how SALP may be used to prevent remote payment assaults even in the absence of a trusted hardware infrastructure, as shown in this research paper. Finally, we argue that the convenience of mobile payment situations is not compromised by SALP since it does not raise system overhead.

Work in [11] did research that dove into this very question. Data-driven anti-fraud engineering for online payment systems benefits greatly from the addition of relevant function modules to increase detection capabilities. This method overcomes the limitations of previous approaches to fraud prevention that focused on a specific function. The need to enhance detection performance, offer understandable decision-making, and reduce processing latency and computing resource utilization are just a few of the tough criteria that make achieving a validated integration difficult. Based on these findings, it is suggested that the CAeSaR certified integration system might be used to meet all of these needs at once. Two cutting-edge approaches work together to get the desired effect. The TRTPT system is the first to use a new three-way taxonomy to classify functions. The classification system relies on the relative timing of transactions in relation to a fictitious transaction used as a point of reference. CAeSaR is able to provide three separate modules for preventing fraud thanks to the Trustworthy and Resilient Transaction Processing Technology (TRTPT). When used together, these modules may successfully counter a wide range of fraudulent activities. TELSI is an efficient method of integration. Integrating judgements from three function modules with only two basic logical connectives successfully achieves choice explainability, leading to the creation of candidate decision procedures. TELSI employs a multi-classification stacking strategy developed to dynamically apply the best appropriate decision method to each individual transaction. Real data from a prominent bank's scenario approach is used to verify CAeSaR's benefits in reality.

Work's (2012) research examines the link between the meteoric rise of cybercrime and the proliferation of online commerce. Detecting online payment fraud is crucial in the dynamic field of electronic commerce since it represents a major obstacle for online businesses. It is widely accepted that behavior-based approaches hold great promise for identifying cases of fraudulent online financial transactions. It is a significant problem to build accurate behavioral models from poor quality behavioral data. In this study, we zero in on improving data quality for behavioral

modeling. We can infer reliable co-occurrence correlations of transactional characteristics using a knowledge network. In addition, heterogeneous network embedding is used to better describe intricate connections. Different network embedding strategies for general agent-based, population-level, and individual-level models of behavior are our core focus. The examination of a real-world dataset taken from a commercial bank shows that our suggested method significantly outperforms the state-of-the-art methods, providing empirical proof for the technique's usefulness. Online banking payment systems might benefit greatly from the use of realistic behavioral models for fraud detection. This research is the first we are aware of that attempts to employ network embedding approaches to improve data augmentation for varied behavior models by analyzing co-occurrence correlations between attributes.

According to the study cited in footnote [13], heterogeneous System-on-Chip (SoC) designs include elements of both FPGAs and CPU cores onto a single chip. This combination is made with the intention of improving the functionality of several programs, including those that use deep learning and encryption. Directly connecting the FPGA and CPU SDRAM allows FPGAs to begin noncacheable synchronous DRAM (SDRAM) transactions. Because FPGAs and CPU cores can pool their resources, this is feasible. Therefore, in the case of malicious conduct, the 3rd party intellectual properties (3PIPs) included into the FPGA are capable of executing SDRAM rowhammer assaults. Existing countermeasures relying on performance counters have limited success in identifying such attacks due to the lack of cache involvement in memory transfers from FPGAs. Existing countermeasures, which track the rate at which memory rows are activated, can't pin down the specific IP used by an attacker's FPGA, making them vulnerable to assault. The SDRAM transactions from IPs on the FPGA destined for each bank of the microprocessor SDRAM may be monitored by our company's security solution, which makes use of the FPGA-to-microprocessor SDRAM link. The FPGA fabric might be used to create the suggested monitoring system. The system can identify an attempt to launch a rowhammer attack, which causes bit flips in the SDRAM, before the attack is launched. It uses 6.3% of the ALMs available in an Intel Cyclone V FPGA while monitoring a large number of IP addresses for several applications.

According to studies published in [14], examining electric network frequency (ENF) may be used as a forensic method for determining whether or not a multimedia recording has been tampered with. For ENF analysis to be successful and reliable, it is crucial that high-quality ENF signals can be reliably extracted from multimedia recordings. In this research, we take a look at two popular techniques for deriving electric network frequency (ENF) signals from visual data captured by rolling-shutter cameras, and we compare and contrast their respective merits and drawbacks. Direct concatenation, the first method presented in the aforementioned study, ignores the downtime between frames. The second method utilized in this research is called periodic zeroing-out, and it consists of adding zeros to the missing sample points to account for the idle time. While the first method does not require precise knowledge of the camera's read-out time in order to extract ENF signals, both empirical testing and theoretical evaluations of using multirate signal processing show that the resulting ENF signals are distorted to varying degrees. The second technique, which uses the read-out time as an additional input, can reliably extract ENF signals with no degradation. The strongest signaling frequency component also tends to coincide with the nominal frequency. We also compare the two approaches by analyzing the aliased direct current (DC) and negative electric network frequency (ENF) components that come from them, and we find that they have a little effect on the precision of frequency estimation. This study aids in comprehending the basic steps necessary to extract video ENF signals. Results show that the periodic zeroing-out technique provides more precise

frequency forecasts. However, it is essential to remember that the magnitude of the performance improvement varies greatly depending on the application or environment.

Password-based authenticated key exchange (PAKE) systems may benefit from using multi-factor authentication, according to studies cited in [15]. It serves as the main line of defense in the security of many popular mobile apps including e-Bank, smart homes, and cloud services. Despite much study, the problem of creating a safe and effective multi-factor authentication system has not been solved. A large number of newly developed systems come with extensive security proofs that prove their efficacy. However, it didn't take long for the majority of these systems to be exposed as vulnerable and unable of delivering on their promised security promises. When a multi-factor system that has been described as "formally proven secure" turns out to be vulnerable, the contradiction is striking. This research is a crucial first step in methodically exploring the flaws in mobile device multi-factor authentication methods and attempting to resolve the apparent contradictions that surround this topic. Let's start with the random oracle model to investigate the root reasons of the absence of "provable security" in unreliable multi-factor authentication systems. Using the five steps of a formal security proof, we will next divide these triggers into eight distinct classes. Then, the eight types of proof failures and their solutions are thoroughly analyzed, and finally, three widely used susceptible methods are analyzed in depth. Finally, we undertake a comprehensive comparison of 70 example multi-factor authentication techniques using our expanded assessment criteria. Comparison findings reveal that knowing the limitations of formal security proofs is helpful in developing multi-factor authentication protocols that offer increased security for mobile devices and settings, and the time span covered by the chosen methods extends from 2009 to 2022.

According to studies such as [16], there are significant obstacles to implementing attribute-based encryption (ABE) systems in cloud storage services (CSS). There is a major roadblock caused by the existence of a central authority responsible for managing all characteristics. The absence of a reliable attribute revocation system that swiftly prohibits illegal access after a request for attribute revocation is the second difficulty. The greatest difficulty comes from avoiding the attribute revocation situation altogether. An approach is proposed in this research to address these issues with CSS. A multi-authority attributes management system that is both powerful and comprehensive is the answer. The suggested system may be built using either the Key Policy Attribute-Based Encryption (KP-ABE) or Ciphertext Policy Attribute-Based Encryption (CP-ABE) method, both of which have their own unique properties. The proposed system also includes a high-level digital identification structure for users, which prevents them from working together. The suggested system's duties may be fulfilled without any coordination among the concerned agencies. In addition, the authorities may choose to participate in or opt out of the proposed system at any time without the need to re-initialize the system. According to the provided performance measures, the suggested system can accomplish the set objectives with sufficient efficiency levels.

Code-based masking is an active subject of study, as seen by the studies in [17], with the goal of creating masking schemes that can be shown to be successful against side-channel assaults. This strategy is useful for expanding and unifying various forms of masking within the framework of a formalization based on coding theory. To a large extent, the amount of side-channel robustness is tuned by the choice of the underlying linear codes in code-based masking methods. The purpose of this study is to examine the repercussions of attack-based assessment on the higher-order optimal distinguisher (HOOD). Information leakage in code-based masking is also being investigated to see whether or not it may be exploited for different scenarios. Shamir's secret sharing (SSS) and inner product masking (IPM) are two

examples of code-based masking that are the subject of this research. Our research shows that the more complex theoretical derivatives are accurate, as shown by the simulated data. Attack-oriented assessments, which evaluate the information's potential for being exploited in an attack, enrich the study even more. Information leakage measurements may be used to draw theoretical conclusions. More specifically, we use 2 and 3 shares in conjunction with (3, 1)-SSS based masking to categorize all possible linear code alternatives in the IPM. Additionally, we rank the best and worst codes in each group. Based on our empirical assessments, we suggest looking into the coding-theoretic features to find the best linear codes for enhancing code-based masking strategies. Regarding applications, our attack-centered assessment technique equips designers with the resources they need to improve the safety of code-based masking by using optimum linear codes. Our research employs a method that uses simulated leakage traces to help with source code validation and patching in the event that vulnerabilities are discovered.

Nonvolatile memories (NVMs) are becoming more popular due to their improved access times, storage capacities, energy efficiency, and scalability. Examples of such NVMs are resistive random-access memory (RRAM) and spin-transfer-torque random-access memory (STTRAM). As a result, they show great potential for several uses involving data storage. However, it has been shown that these technologies reveal the Hamming weight of data through a power side-channel when executing read and write operations. We suggest a technique that makes use of the voltage regulator (VR) and on-chip capacitor to ease read/write operations on NVMs. By cutting off power to the memory array during writes and reads, we can eliminate any potential for leakage via a side channel. Reducing the potential for data loss during capacitor refilling necessitates a thorough and secure discharge of any remaining charge in the capacitor bank. The capacitor will deplete throughout the read/write process, but the voltage regulator (VR) will keep the voltage stable. The design's performance decreases when measured against the parsec and splash-2 benchmarks, by anywhere from 0.53% to 1.2% in terms of instructions per cycle. Space and power overheads of 3.54105105 and 3.05105105 respectively are incurred when a 4-Mb RRAM memory array is implemented. A 64-bit word's security may be improved by a factor of between 2.7 x 1019 and 264 using the suggested technique. SecNVM in memory macros are highly recommended for guaranteeing security while keeping operating expenses low. SecNVM is a flexible solution that can shield cryptographic engines and other security modules against power-side-channel assaults.

According to [19], an all-encompassing security solution was offered to protect smart meters from threats that may compromise their critical electrical components. The theft of electricity by hacking into smart meters accounts for a significant fraction of these incidents. It is possible for an antagonistic party to tamper with or replace parts of a system that carry out measuring operations or store vital data. Attacks on smart meters are common since they are placed in precarious locations and may be easily accessed by criminals. As a result, it is crucial to create effective methods to prevent unauthorized people from physically tampering with smart meters. Our method takes use of the material characteristics of these parts to generate trustworthy meter IDs. We highlight our two most significant contributions. The first strategy is motivated by the need for physically unclonable capabilities and relies on the separation of identities in SRAM modules. Then, a strong identity is constructed by fusing the many parts. The smart meter's voltage levels provide physical context data that may be used to generate dynamic context identities, which is the second contribution. Experiments are performed on a hardware prototype consisting of voltage sensors, SRAM memory, and Arduino microprocessors in order to provide empirical confirmation of the principles. The research shows that our suggested method can successfully shield smart meters against component-

level assaults and is practical enough for widespread deployment.

Previous studies have investigated the development of smart cities and the related technical advances, emphasizing their emergence as fascinating study topics. In smart cities, 5G networks are crucial for identity identification, online banking, and cyber security via intelligent access management. To prevent identity theft and other forms of fraud in an online environment, it is crucial to have strong authentication procedures. Many intelligent application domains need stringent security measures due to the widespread use of biometric modalities like fingerprints for identification and authentication purposes. Our research recommends a technique for detecting shifts in biometric modalities as a way of distinguishing between authentic, manipulated, and false biometrics in 5G-enabled smart cities. A three-stage likelihood calculation is carried out to determine the possibility of biometric manipulation. Deep learning methods, especially convolutional neural networks (CNN) and a hybrid model that combines CNN with convolutional long-short term memory (ConvLSTM), are used in this computation. Experiments conducted in a simulated environment show that the accuracy of alteration detection is on par with more sophisticated methods when it comes to identifying shifts in the fingerprints' central rotation. Several biometric authentication applications might benefit from the deployment of the suggested method in secure smart cities.

Scholarly investigations have emphasized the importance of mobile devices in the modern world, showing how they have become practically indispensable [21]. The increasing use of mobile devices has piqued interest in mobile banking. Some of the most well-known examples are WeChat Pay, Apple Pay, and Google Wallet. However, a sizable percentage of these technologies are created with the main aim of enabling customer payments to the business. The business-to-user model was crucial to the development of these companies. Furthermore, either the payer or the payee must maintain an active network connection with an external payment server for the duration of the transaction. Our work aims to improve upon current methods by enabling dual-anonymous, offline payment systems. The BBS+ signature method is proposed as a means to launch a dual-anonymous offline electronic currency. Our method includes dual-anonymous payment, in which both parties to a transaction may stay anonymous to one another, even if all other users and the payment server are in on a secret plot to reveal their identities. We also employ performance analysis and a formal proof of security to show that the proposed scheme's security can be derived on the basis of commonly accepted assumptions. We further prove that the approach may be used in m-commerce implementations.

Research published in [22] indicates that the rapid development of cloud-enabled IIoT in healthcare has led to considerable savings in the cost of home monitoring and safety assurance. In addition, the quality of medical treatment has increased significantly. The authenticity, tamper resistance, and bilateral fine-grained access control of shared health data raises special security and privacy issues despite its numerous advantages and conveniences. To remedy these drawbacks, this research proposes PBAC-FG, a safe privacy-preserving bilateral access control mechanism with fine granularity. To allow participants like patients and healthcare providers to create customized access control settings for their encrypted health data, the PBAC-FG uses matchmaking encryption and fine-grained access control techniques. In this way, sensitive medical information is protected from unauthorized eyes. Further, in order to verify our PBAC-FG's security, it is advised that we do extensive security proofs. We conduct in-depth performance evaluations and comparisons to prove the viability and use of the PBAC-FG in the context of IIoT healthcare applications.

The study cited in footnote [23] predicts that IoTs will have a major effect on the logistics and transportation service industry in the next years. Increased security risks and considerable financial issues have come from

the incorporation of pervasive Internet of Things (IoT) technology into maritime transportation systems (MTS). When connected to MTS networks, Internet of Things (IoT) items are at risk from the Distributed Denial of Service Attack (DDoS). Timely and accurate identification of such risks is crucial for successful mitigation strategies. Traditional methods for detecting and diagnosing Distributed Denial of Service (DDoS) attacks rely on the idea of entropy in network data properties. However, the vast majority of these approaches are static in nature, taking into account just a select few aspects of network traffic. This constraint thus limits the range of possible Distributed Denial of Service (DDoS) attack types and sizes that may be properly recognized. Using three different window widths and the related Rate of Exponent Separation (RES), a new system called "Dual Stack Machine Learning (S2ML)" has been presented to produce different entropy-based variable 10-Tuple (T) features from network traffic data. Using MTS-IoT information, we have built a complex model that accurately predicts the occurrence of DDoS assaults based on the aforementioned characteristics. Using Multi-layer Perceptron (MLP), Alternating Decision Tree (ADT), and Simple Logistic Regression (SLR), a comparative study demonstrates the S2ML framework's efficacy in overcoming the shortcomings of traditional DDoS detection methods. Confusion metrics and ROCs are only two of the numerous assessment metrics included in this investigation. Results for normal/attack traffic distribution may be improved upon by an extra 1.5% when the S2ML algorithm is utilized instead of the described tactics. Improving the model's efficiency requires using dynamic windowing methods, keeping an eye on packet loss rates, and adopting a Software Defined Networks (SDNs) architecture.

Direct Anonymous Attestation (DAA) is a cryptographic approach that, according to the research described in reference [24], makes it easier to create anonymous signatures. This approach was developed so that the Trusted Platform Module (TPM), a tiny piece of hardware permanently installed in a host computer, could offer proof on the integrity of the host system without endangering the user's privacy. Fully anonymous signatures and pseudonymous signatures are two of the signing methods made available by DAA. Because of the TPM's limited resources, one of the main focuses of Direct Anonymous Attestation (DAA) research is finding ways to lessen the TPM's workload when it comes to signing documents. Within a perfect DAA framework, the TPM's signing effort won't go above and beyond what's needed for a regular signature scheme like ECSchnorr. The current state of document signing systems is far from ideal for any signature style. This research proposes the first DAA method that provide optimum TPM signing efficiency across both signature modalities. In this method, a signature is generated by having the Trusted Platform Module (TPM) do a single exponentiation. This specific exponentiation may have already been calculated, which is something to keep in mind. The suggested technique is compatible with the TPM 2.0 specification since it may be carried out using the current TPM 2.0 directives. We put an Infineon TPM 2.0 chip through its paces by testing the TPM 2.0 instructions required in three distinct deployments of DAA. Our DAA technique's host signature and verification algorithm ran on a laptop with a 1.80GHz Intel Core i7-8550U processor. Our experimental results show that our Dynamic Adaptive Authentication (DAA) method takes around 144 ms to sign in both modes combined. When compared to the current DAA approaches permitted by TPM 2.0, our scheme displays a better degree of signing efficiency; nevertheless, with the use of pre-computation, we are able to obtain a reduced signing time of roughly 65 ms. When compared to existing methods, ours is nearly twice as fast when it comes to online signing efficiency and almost five times faster when it comes to overall signing efficiency levels.

As detailed in reference [25], academic work is now ongoing to build a learning-based safe control framework for cyber-physical systems in an effort to solve sensor and actuator problems. In this research,

we suggest using a collection of observer-based estimators and a threat-detection level function to detect and prevent assaults. A nominal-feedback controller is used when operating circumstances are ideal. The accuracy of the readings is verified by using the suggested attack monitoring techniques. Two players, the defense and the attacker, take part in a differential gaming process. The defender's position in this game is that of the minimizer, whereas the attacker's is that of the maximiser. The goal of the attacker is to compromise a subset of the sensors and/or actuators by injecting attack signals into them. The primary difficulty of joint state estimation and attack mitigation is then tackled using a reinforcement learning approach, leading to the development of a safe control policy for different scenarios. The effectiveness of the suggested frameworks is shown with two numerical examples. An empirical survey of these methods can be observed from the next section of this text.

III. RESULT ANALYSIS & COMPARISON

From the in-detail review of existing models, it can be observed that these models vary widely in terms of their real-time performance levels. In this section, the performance of these methods is compared in terms of Precision (P), Accuracy (A), Complexity (C), Deployment Cost (DC), and Scalability Metrics. These parameters are evaluated on an Iterative scale from 1 to 10 in table 1 as follows

Table 1. Comparative Analysis of Different Models

Method	Reference Number	Precision	Accuracy	Complexity	Deployment Cost	Scalability
Dual-anonymous off-line electronic cash scheme using BBS+ signature	[1]	8	9	6	3	7
Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)	[2]	9	8	4	3	9
Dual Stack Machine Learning (S2ML) framework for DDoS attack detection	[3]	8	8	6	3	9
Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency	[4]	9	9	3	3	9
Learning-based secure control framework for	[5]	9	9	8	5	9

cyber-physical systems with attack detection and mitigation						
Behavioral modeling for fraud detection using network embedding	[6]	8	8	8	3	9
Integration of function modules for anti-fraud engineering in online payment systems	[7]	9	9	8	4	9
Research into the link between cybercrime rise and online commerce growth	[8]	8	8	6	3	7
Heterogeneous System-on-Chip (SoC) designs with FPGA and CPU for improved functionality	[9]	8	8	6	4	9
Electric network frequency (ENF) analysis for multimedia tampering detection	[10]	8	8	4	3	9
Challenges and improvements in multi-factor authentication systems for mobile devices	[15]	9	9	8	4	9
Challenges and solutions in implementing attribute-based encryption in cloud storage	[16]	9	9	8	3	9
Code-based masking for counteracting side-channel attacks	[17]	9	9	8	4	9

Security strategy for protecting smart meters against component attacks	[18]	9	9	8	3	9
Emerging nonvolatile memory technologies and their power side-channel vulnerabilities	[19]	9	9	8	4	9
Security of biometric modalities in 5G-based smart cities	[20]	9	9	8	3	9
Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)	[22]	9	9	4	3	9
Dual Stack Machine Learning (S2ML) framework for DDoS attack detection	[23]	8	8	6	3	9
Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency	[24]	9	9	3	3	9
Learning-based secure control framework for cyber-physical systems with attack detection and mitigation	[25]	9	9	8	4	9

Numerous techniques provide excellent precision ratings, demonstrating their capacity to deliver reliable findings with few false positives. Methods such as [2] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [4] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", [5] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation", [7] "Integration of function modules for anti-fraud engineering in online payment systems", [15] "Challenges and improvements in multi-factor authentication systems for mobile devices", [16] "Challenges and solutions in implementing attribute-based encryption in cloud storage", [17] "Code-based masking for counteracting side-channel attacks", [18] "Security strategy for protecting smart meters against

component attacks", [19] "Emerging nonvolatile memory technologies and their power side-channel vulnerabilities", [20] "Security of biometric modalities in 5G-based smart cities", [22] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [24] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", and [25] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation" all achieve the highest precision score of 9. As a result, it can be inferred that these techniques are efficient at delivering exact results and are suitable for use in situations where accurate identification and classification are necessary.

Numerous techniques have excellent accuracy ratings, demonstrating their general ability in producing accurate findings. These methods include [1] "Dual-anonymous off-line electronic cash scheme using BBS+ signature", [3] "Dual Stack Machine Learning (S2ML) framework for DDoS attack detection", [4] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", [5] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation", [6] "Behavioral modeling for fraud detection using network embedding", [7] "Integration of function modules for anti-fraud engineering in online payment systems", [9] "Heterogeneous System-on-Chip (SoC) designs with FPGA and CPU for improved functionality", [10] "Electric network frequency (ENF) analysis for multimedia tampering detection", [15] "Challenges and improvements in multi-factor authentication systems for mobile devices", [16] "Challenges and solutions in implementing attribute-based encryption in cloud storage", [17] "Code-based masking for counteracting side-channel attacks", [18] "Security strategy for protecting smart meters against component attacks", [19] "Emerging nonvolatile memory technologies and their power side-channel vulnerabilities", [20] "Security of biometric modalities in 5G-based smart cities", [22] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [23] "Dual Stack Machine Learning (S2ML) framework for DDoS attack detection", [24] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", and [25] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation", with accuracy scores ranging from 8 to 9. These techniques are excellent candidates for security applications where accuracy is essential since they are likely to provide trustworthy and accurate results.

Higher complexity ratings for certain approaches imply that sophisticated implementation or analysis procedures may be involved. Methods such as [4] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", [5] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation", [6] "Behavioral modeling for fraud detection using network embedding", [7] "Integration of function modules for anti-fraud engineering in online payment systems", [8] "Research into the link between cybercrime rise and online commerce growth", [9] "Heterogeneous System-on-Chip (SoC) designs with FPGA and CPU for improved functionality", [15] "Challenges and improvements in multi-factor authentication systems for mobile devices", [16] "Challenges and solutions in implementing attribute-based encryption in cloud storage", [17] "Code-based masking for counteracting side-channel attacks", [18] "Security strategy for protecting smart meters against component attacks", [19] "Emerging nonvolatile memory technologies and their power side-channel vulnerabilities", [20] "Security of biometric modalities in 5G-based smart cities", [23] "Dual Stack Machine Learning (S2ML) framework for DDoS attack detection", [24] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", and [25] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation" have complexity scores of 8. These techniques could call either deep

technical knowledge or complicated algorithms, perhaps making them more appropriate for circumstances where difficult security concerns must be solved for different use cases.

Numerous techniques have relatively low deployment cost ratings, which shows that putting them into use will save money. Methods like [1] "Dual-anonymous off-line electronic cash scheme using BBS+ signature", [2] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [3] "Dual Stack Machine Learning (S2ML) framework for DDoS attack detection", [4] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", [8] "Research into the link between cybercrime rise and online commerce growth", [10] "Electric network frequency (ENF) analysis for multimedia tampering detection", [15] "Challenges and improvements in multi-factor authentication systems for mobile devices", [16] "Challenges and solutions in implementing attribute-based encryption in cloud storage", [18] "Security strategy for protecting smart meters against component attacks", [20] "Security of biometric modalities in 5G-based smart cities", [22] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [23] "Dual Stack Machine Learning (S2ML) framework for DDoS attack detection", [24] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", and [25] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation" achieve deployment cost scores of 3 or 4. These techniques are probably appealing choices for enterprises wishing to adopt reliable security solutions without bearing a disproportionate cost loads. All approaches have excellent scalability ratings, demonstrating their ability to successfully manage growth and development process. These approaches have scalability ratings of 9, indicating that they can handle growing demands while maintaining performance as systems become bigger for different use cases. In the ever-changing and dynamic world of financial situations, this quality is crucial for real-time scenarios.

Thus, techniques [4] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", [5] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation", [7] "Integration of function modules for anti-fraud engineering in online payment systems", [15] "Challenges and improvements in multi-factor authentication systems for mobile devices", [16] "Challenges and solutions in implementing attribute-based encryption in cloud storage", [17] "Code-based masking for counteracting side-channel attacks", [18] "Security strategy for protecting smart meters against component attacks", [19] "Emerging nonvolatile memory technologies and their power side-channel vulnerabilities", [20] "Security of biometric modalities in 5G-based smart cities", [22] "Secure privacy-preserving bilateral access control scheme with fine granularity (PBAC-FG)", [24] "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency", and [25] "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation" emerge as consistently strong performers across multiple parameters. They are potentially good options for boosting security in banking systems because to their great precision, accuracy, and scalability, as well as reasonable complexity and implementation costs. To make an educated choice, it is vital to have a complete grasp of the approaches and how they correspond with particular banking security needs for different scenarios.

IV. Conclusion and future scope

To address the essential need for strong security paradigms in the face of increased cyber threats and rising digitalization, we have analyzed a wide range of security solutions in the context of banking situations

in this thorough investigation. Based on important factors such precision, accuracy, complexity, deployment cost, and scalability, our research has offered a discerning comparative evaluation of various methodologies.

Our analysis's findings show that a few of strategies consistently rank among the best in many different areas. A high degree of precision, accuracy, and scalability is consistently demonstrated by techniques like "Direct Anonymous Attestation (DAA) with optimal TPM signing efficiency," "Learning-based secure control framework for cyber-physical systems with attack detection and mitigation," "Integration of function modules for anti-fraud engineering in online payment systems," and others. These techniques also balance complexity and implementation costs, making them excellent choices for enhancing the security framework of financial organizations.

V. Future Aims

While shedding light on the present state of security models in banking, this study also paves the way for more investigation and advancement in this crucial area. Several places scream out for further investigation:

1. Emerging Technologies: The security environment will change as technology advances. Investigating the integration of cutting-edge technologies like quantum cryptography, artificial intelligence, and blockchain might result in novel security techniques adapted to the particular requirements of banking situations.

2. Adaptive Security: It is crucial to create security models that can dynamically adjust to changing cyberthreats. Unparalleled protection may be possible via research on adaptive security methods that can identify and block new attack routes in real-time.

3. Usability and User Experience: Although our research focuses on technological issues, future work may explore ways to improve how security measures are used. It continues to be difficult to strike a compromise between strong security and user ease.

4. Regulatory Compliance: Banking institutions must comply with a wide range of rules. Future studies might examine how security models fit with legal specifications, assisting institutions in successfully navigating compliance issues.

5. Sharing threat information: Sharing threat intelligence across financial organizations might result in more comprehensive security measures. It would be beneficial to look at how security models might enable efficient information exchange while protecting privacy levels.

Our study's findings highlight the urgent need for advanced security models in the banking industry. We seek to provide stakeholders, decision-makers, and practitioners with useful insights to strengthen the security fabric of banking operations in an ever-evolving digital ecosystem by identifying high-performing methodologies and outlining future scopes.

VI. REFERENCES

[1] M. Hajiabbasi, E. Akhtarkavan and B. Majidi, "Cyber-Physical Customer Management for Internet of Robotic Things-Enabled Banking," in IEEE Access, vol. 11, pp. 34062-34079, 2023, doi: 10.1109/ACCESS.2023.3263859.

[2] L. Xue, D. Liu, J. Ni, X. Lin and X. S. Shen, "Enabling Regulatory Compliance and Enforcement in Decentralized Anonymous Payment," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 931-943, 1 March-April 2023, doi: 10.1109/TDSC.2022.3144991.

[3] X. Yang, Z. Wang and C. Wang, "Cryptanalysis of a Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile

Payments," in IEEE Systems Journal, vol. 17, no. 1, pp. 601-604, March 2023, doi: 10.1109/JSYST.2022.3171258.

[4] C. Bai, Q. Han, G. Mezzour, F. Pierazzi and V. S. Subrahmanian, "$\sf{DBank}$DBank: Predictive Behavioral Analysis of Recent Android Banking Trojans," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1378-1393, 1 May-June 2021, doi: 10.1109/TDSC.2019.2909902.

[5] M. M. Islam, M. K. Islam, M. Shahjalal, M. Z. Chowdhury and Y. M. Jang, "A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency With Consortium Blockchain: Joint Digital Currency," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 1616-1629, 1 May-June 2023, doi: 10.1109/TSC.2022.3207224.

[6] Z. Qiao, Q. Yang, Y. Zhou and M. Zhang, "Improved Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments," in IEEE Systems Journal, vol. 16, no. 2, pp. 1842-1850, June 2022, doi: 10.1109/JSYST.2020.3046450.

[7] C. Wang, C. Wang, H. Zhu and J. Cui, "LAW: Learning Automatic Windows for Online Payment Fraud Detection," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2122-2135, 1 Sept.-Oct. 2021, doi: 10.1109/TDSC.2020.3037784.

[8] S. S. Ahamad, "A Novel NFC-Based Secure Protocol for Merchant Transactions," in IEEE Access, vol. 10, pp. 1905-1920, 2022, doi: 10.1109/ACCESS.2021.3139065.

[9] N. Ivanov and Q. Yan, "AutoThing: A Secure Transaction Framework for Self-Service Things," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 983-995, 1 March-April 2023, doi: 10.1109/TSC.2022.3185114.

[10] L. Fang et al., "A Secure and Authenticated Mobile Payment Protocol Against Off-Site Attack Strategy," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3564-3578, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3102099.

[11] C. Wang, S. Chai, H. Zhu and C. Jiang, "CAeSaR: An Online Payment Anti-Fraud Integration System With Decision Explainability," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2565-2577, 1 May-June 2023, doi: 10.1109/TDSC.2022.3186733.

[12] C. Wang and H. Zhu, "Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 301-315, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2991872.

[13] R. Elnaggar, S. Chen, P. Song and K. Chakrabarty, "Securing SoCs With FPGAs Against Rowhammer Attacks," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 7, pp. 2052-2065, July 2022, doi: 10.1109/TCAD.2021.3102004.

[14] J. Choi, C. -W. Wong, H. Su and M. Wu, "Analysis of ENF Signal Extraction From Videos Acquired by Rolling Shutters," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4229-4242, 2023, doi: 10.1109/TIFS.2023.3287132.

[15] Q. Wang and D. Wang, "Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 597-612, 2023, doi: 10.1109/TIFS.2022.3227753.

[16] I. M. Ibrahim, M. G. M. Mostafa, S. H. N. El-Din, R. Elgohary and H. Faheem, "A Robust Generic Multi-Authority Attributes Management System for Cloud Storage Services," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 435-446, 1 April-June 2021, doi: 10.1109/TCC.2018.2867871.

[17] W. Cheng, S. Guilley and J. -L. Danger, "Information Leakage in Code-Based Masking: A Systematic Evaluation by Higher-Order Attacks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1624-1638, 2022, doi: 10.1109/TIFS.2022.3167914.

[18] K. Nagarajan, F. U. Ahmed, M. N. I. Khan, A. De, M. H. Chowdhury and S. Ghosh, "SecNVM: Power Side-Channel Elimination Using On-Chip Capacitors for Highly Secure Emerging NVM," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 8, pp. 1518-1528, Aug. 2021, doi: 10.1109/TVLSI.2021.3087734.

[19] A. E. R. Rincón, W. S. Melo, C. M. de Farias and L. F. R. C. Carmo, "Securing Smart Meters Through Physical Properties of Their Components," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-11, 2021, Art no. 3000511, doi: 10.1109/TIM.2020.3041098.

[20] A. Sedik et al., "Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities," in IEEE Access, vol. 9, pp. 94780-94788, 2021, doi: 10.1109/ACCESS.2021.3088341.

[21] J. Ni, M. H. Au, W. Wu, X. Luo, X. Lin and X. S. Shen, "Dual-Anonymous Off-Line Electronic Cash for Mobile Payment," in IEEE Transactions on Mobile Computing, vol. 22, no. 6, pp. 3303-3317, 1 June 2023, doi: 10.1109/TMC.2021.3135301.

[22] J. Sun, Y. Yuan, M. Tang, X. Cheng, X. Nie and M. U. Aftab, "Privacy-Preserving Bilateral Fine-Grained Access Control for Cloud-Enabled Industrial IoT Healthcare," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6483-6493, Sept. 2022, doi: 10.1109/TII.2021.3133345.

[23] F. Ali, S. Sarwar, Q. M. Shafi, M. Iqbal, M. Safyan and Z. U. Qayyum, "Securing IoT Based Maritime Transportation System Through Entropy-Based Dual-Stack Machine Learning Framework," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2482-2491, Feb. 2023, doi: 10.1109/TITS.2022.3177772.

[24] K. Yang, L. Chen, Z. Zhang, C. J. P. Newton, B. Yang and L. Xi, "Direct Anonymous Attestation With Optimal TPM Signing Efficiency," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2260-2275, 2021, doi: 10.1109/TIFS.2021.3051801.

[25] Y. Zhou, K. G. Vamvoudakis, W. M. Haddad and Z. -P. Jiang, "A Secure Control Learning Framework for Cyber-Physical Systems Under Sensor and Actuator Attacks," in IEEE Transactions on Cybernetics, vol. 51, no. 9, pp. 4648-4660, Sept. 2021, doi: 10.1109/TCYB.2020.3006871.

[26] Shivadekar, S., Kataria, B., Limkar, S. et al. Design of an efficient multimodal engine for preemption and post-treatment recommendations for skin diseases via a deep learning-based hybrid bioinspired process. Soft Comput (2023).

[27] Shivadekar, Samit, et al. "Deep Learning Based Image Classification of Lungs Radiography for Detecting COVID-19 using a Deep CNN and ResNet 50." International Journal of Intelligent Systems and Applications in Engineering 11.1s (2023): 241-250.

[28] P. Nguyen, S. Shivadekar, S. S. Laya Chukkapalli and M. Halem, "Satellite Data Fusion of Multiple Observed XCO2 using Compressive Sensing and Deep Learning," IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, Waikoloa, HI, USA, 2020, pp. 2073-2076, doi: 10.1109/IGARSS39084.2020.9323861.

[29] Banait, Satish S., et al. "Reinforcement mSVM: An Efficient Clustering and Classification Approach using reinforcement and supervised Techniques." International Journal of Intelligent

Systems and Applications in Engineering 10.1s (2022): 78-89.

[30] Shewale, Yogita, Shailesh Kumar, and Satish Banait. "Machine Learning Based Intrusion Detection in IoT Network Using MLP and LSTM." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 210-223.

[31] Vanjari, Hrishikesh B., Sheetal U. Bhandari, and Mahesh T. Kolte. "Enhancement of Speech for Hearing Aid Applications Integrating Adaptive Compressive Sensing with Noise Estimation Based Adaptive Gain." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 138-157.

[32] Vanjari, Hrishikesh B., and Mahesh T. Kolte. "Comparative Analysis of Speech Enhancement Techniques in Perceptive of Hearing Aid Design." Proceedings of the Third International Conference on Information Management and Machine Intelligence: ICIMMI 2021. Singapore: Springer Nature Singapore, 2022

Cite this article as :

Suraj Pawar, Prof. Abhimanyu Dhutonde, "An In-Depth Analysis of & Performance Comparison Security Models Used In Banking Scenario", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.10-29, September-October-2023.