Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2024, 11(6):55-62**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Secure Data Transmission and Storage for Data Security in Banking Using Reporting Tools

Pranay Mungara

Sr. Data Analyst, Business Intelligence, Virtusa Corporation, USA
Email ID: pranay.mungara@gmail.com

Abstract Providing protection for Internet-enabled devices that connect to remote networks is a primary focus of security on the Internet of Things (IoT). Internet of Things (IoT) Safety is a security component that tries to prevent cybercriminals from compromising IoT devices and frameworks, making it an integral part of the IoT. The banking applications, on the other hand, are being dynamically regulated since they are unable to provide an appropriate degree of customer service, as well as protect themselves against digital attacks and respond to them. One of the most important factors contributing to this is the susceptibility of organisations and systems in the financial technology sector to malfunction. Therefore, wireless organisations that cover these Internet of Things gadgets are exposed to a significant lack of protection. Because the Internet of Things is a lightweight architecture, it is suited for use in situations where lightweight and energy-efficient cryptography is being utilised for assurance. Steganography and hybrid algorithms were also studied as part of this research. According to the findings of this research, the Advanced Encryption Standard is the standard that is most often used for mobile banking. This is due to the fact that there have been no particular attacks launched against it up until this point. The Advanced Encryption Standard, on the other hand, might not be able to guarantee the safety of mobile banking for very long because of the rapid pace of technological advancement. Therefore, this study exposes and proposes a hybrid method that is resistant to flaws in current cryptosystems by combining the Advanced Encryption Standard algorithm with Least Significant Bit steganography.

Keywords Data Security, Data Transmission, Storage, Banking

Introduction

Mobile banking apps, sometimes referred to as M-banking, allow users to establish online conversations with financial institutions whenever and wherever they choose [1]. Banks and other financial organisations have begun offering their customers remote access to their accounts through the use of platforms like mobile banking apps. Several banking services, including as checking account balances, transferring funds, and buying and selling stocks, are available to users through mobile banking [2]. Additional services offered by m-banking include the ability to top off airtime, pay off loans, and make reservations. Banks and their clients alike can reap the benefits of mobile banking since it gives users secure remote access to services whenever they need them, regardless of the time of day or night [3]. Mobile banking has the potential to boost competitiveness while cutting operational costs [4].

Mobile devices and wireless networks allow for the transmission of sensitive financial data, including transactions and account information (usernames, passwords, and personal identification numbers). You may access your financial services from anywhere thanks to this. Be that as it may, mobile banking isn't completely secure due to a number of issues [5]. Mobile banking facilities are frequently targeted by threats like eavesdropping, malware, phishing, denial of service, and unauthorised access, among others. The great bulk of these assaults occur on insecure networks. Several techniques, including steganography and encryption algorithms, can be employed to prevent unauthorised individuals from accessing client accounts [6].

Several various kinds of encryption algorithms, steganography, and hybrid techniques were discussed in this study. These algorithms can be utilised to protect user data while it is in transit in mobile banking. The evaluation found that the Advanced Encryption Standard (AES) algorithm offered the highest level of security for mobile banking. This is because it has not been compromised and can encrypt and decode data quickly. The fast

development of new technologies, however, makes it likely that AES may fail to uphold its fundamental security principle [7]. Considering this, the results of this study show that a combination of Advanced Encryption Standard (AES) encryption with a steganography method, like Least Significant Bit (LSB), can add an extra degree of protection. This is because LSB steganography brings security properties like embedding a message within an image, but the Advanced Encryption Standard (AES) algorithm adds features like encryption and decryption through the use of a key. This makes the developed hybrid technique impenetrable to tampering; even if an adversary were to use publicly available software to detect a message in the image, they would still not be able to deduce the encryption key used to decipher it. The findings of this study highlight the importance of mobile banking service providers implementing robust security measures to prevent unauthorised access to customer data while it is in transit [8]. Because of this step, fraudsters will have a harder time breaking into customers' bank accounts and stealing their money and personal details. Decisions regarding the creation of mobile banking applications—which clients use to access banking services remotely—must be based on the information gleaned from this article.

Secure Storage for Banking Apps That Are Based in The Cloud

A crucial requirement for carrying out high-end data transfers in current contemporary era is the utilisation of encrypted communication. Despite the fact that it is becoming increasingly prevalent in the banking industry, the secure cloud storage mechanism is still in its infancy. The banking storage mechanism is a source of concern because it demands immediate attention. Reasons such as rewards, security, confidentiality, viewpoint, usability, data management, unpredictable growth in transaction volume, and cost reduction necessitate this focus. Software as a service (SaaS) is one way that cloud computing provides XaaS to the banking industry. Accounting, customer relationship management, invoicing, and corporate resource planning are all helped out by this sort of software-as-a-service (SaaS).

Applications can run on a platform that is suitable for PaaS. It is helpful in lowering the cost of the information technology infrastructure, and it may also greatly reduce the amount of money spent on hardware devices and software applications. With the use of LaaS, companies can buy those assets as a redistribution service. A similar strategy is employed for the safe use of a cloud storage mechanism that includes XML Web services and a logging mechanism in order to give an overview of the SSL VPN's architecture. In this way, we can keep an eye on what users are up to and find security flaws before they happen. Also, it's a secure ECC storage method that's used in transaction-rich applications (TRA). Storage mechanism 4's many advantages, including its service-oriented architecture and smooth accessibility, have led many TRAs to adopt it.

Nevertheless, it is susceptible to being hacked and being attacked by threats. As a result, the protection of this environment is of the utmost significance, and several study activities that are centred on this topic are being reported. When it comes to managing sensitive financial data in the cloud, the security measures offered by cloud service providers are insufficient. When it comes to funding activities like payroll, accounting, CRM, invoicing, enterprise resource planning, and related processes, both the client and the banking industry are seeking for increased protection.

Assurance of safety Those working in the financial industry will not tolerate any breaches. In the context of the cloud computing ecosystem present today. The only layer of security that TRA possesses is a single one. Therefore, it is necessary to have a system that can give high-level security while also saving money, having good performance, and having bandwidth. The given solution is designed to provide a high-level design of the SSLVPN with ECC. This design can then be implemented to a private cloud with a secure logging system.

Using the Microsoft Azure cloud platform, the approach has worked with Java programming and an open virtual private network (VPN). For the purpose of performance analysis, a SOAP UI tool has been utilised, and this tool has been installed into the cloud web server [9].

A private cloud environment was also included in the design's implementation, along with a tailored secure logging system that will be encrypted using ECC. This safeguarded the confidentiality of user information and prevented unauthorised access to their cloud-based activities. Initiating the ECC-based SSL VPN application requires the system to incorporate the private cloud VPN frameworks.

The identical strategy is utilised in the cloud storage system for the TRA (banking) customers, meaning that they are able to obtain a great deal of advantages [10].

- Utilisation of Time: Customers are able to utilise it at any time, day or night.
- Banks can benefit from the enhancement of their adaptability through the promotion of adaptability ratios and operating leverage [11].
- Reduce the Amount of Money Is Invested: The financial institutions are not prepared to invest a significant amount of money in order to acquire software, hardware, and manpower that is associated with cloud computing.

• When compared to online and internet banking put together, the security precautions of the ECC-based secure cloud storage mechanism for TRA are much more robust.

ECC is an extra safeguard that this service offers. The banking customer adds an extra layer of protection to the peer-to-peer network by connecting it to the cloud and using SSL and ECC simultaneously [12]. Not only that, but the banking app also uses the identical ECC digital keys.

Information And Communication Technology Security

Recent global security incidents have made it abundantly evident that cyber security risks are growing in both complexity and severity. Attackers are become more coordinated, and automation is allowing them to use more advanced methods and tools in their assault vectors. The primary barrier to preventing cyberattacks is raising public and professional awareness of the need of security measures. Doing so ensures that security personnel are up-to-date on the latest attack tactics and technology and can respond accordingly. Participants in these training sessions have access to cyber security laboratories and activities. Cyber security exercises are typically described as training exercises that include the execution of attack and defence scenarios on both virtual and physical environments.

The purpose of the exercise is to improve the participants' understanding of attack and/or defence, as well as their skills in these areas. The planning and execution of such exercises include participation from a variety of different groups of individuals. The training environment is created by a group of individuals who are collectively referred to as the white team. There is another squad that actively seeks for environmental weaknesses; they call themselves the red team. On the other hand, the blue team is responsible for protecting the environment and warding off any potential threats.

Those who are participating in an exercise are expected to fulfil these primary fundamental duties. Following this, we will go over a more exhaustive description of all the responsibilities that are involved in an exercise. I would like to bring to your attention that we refer to any activity that involves practical training or awareness as a security exercise.

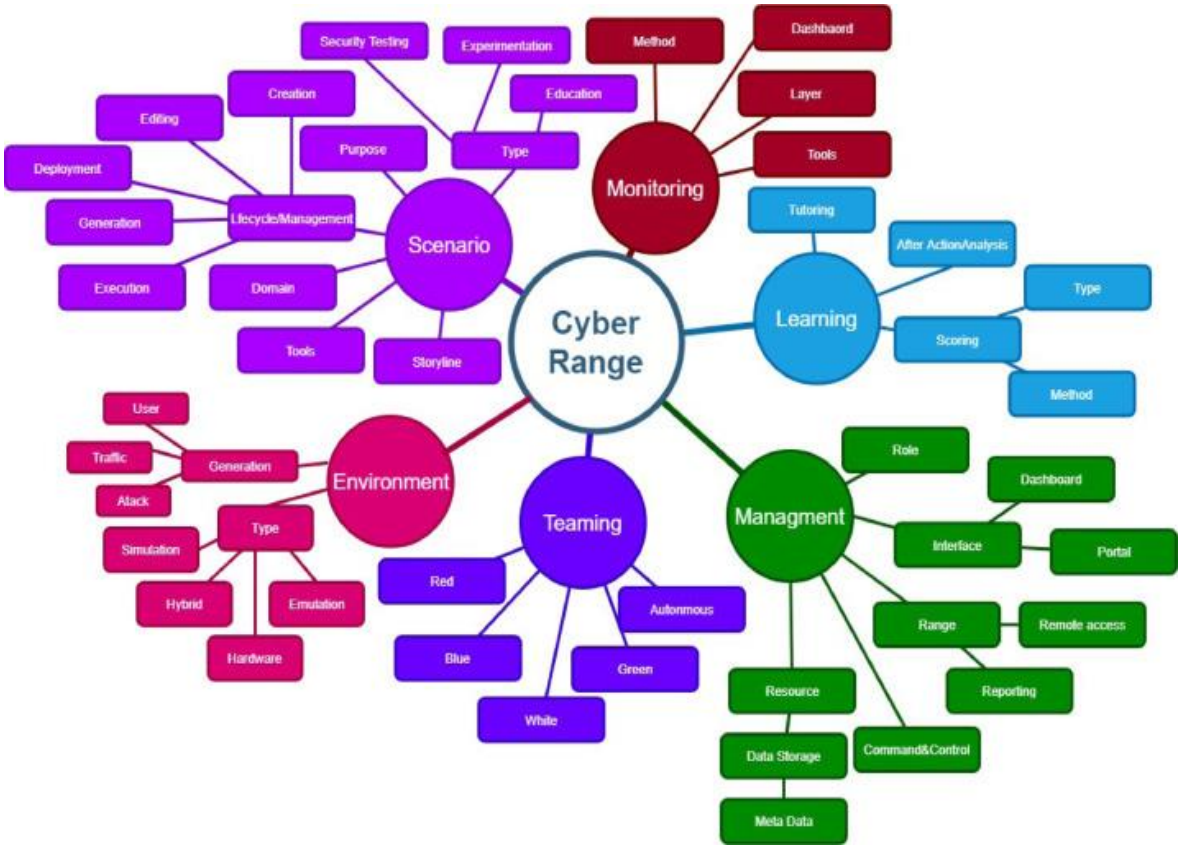

Figure 1: Cyber ranges and security testbeds

Protecting oneself from cybercrimes and threats begins with being aware of the risks and being prepared to respond. Information security training is one line of defence against these threats. Two distinct kinds of instruction

are available. Security personnel are the target of the first kind of training, which aims to update their knowledge of current threats and strengthen their defences and mitigation strategies. This endeavour aims to do more than just research on cyber ranges; it will also thoroughly review the literature on unclassified cyber ranges and safety test beds [13].

In this review, we build a taxonomy for cyber range systems and examine the current literature, which covers a wide range of subjects including design, scenarios, capacities, functions, resources, and more. This article assesses the advantages and disadvantages of a smart grid that relies on the Internet of Things (IoT). This article takes a close look at the smart grid's cyber-security environment and focuses on various cyber risks. We zero in on network weaknesses, analyse them, and then introduce protection requirements while simultaneously challenging workarounds. A thorough understanding of cyber-security vulnerabilities and solutions is our primary objective, but we also aim to pave the way for future study in this area as it pertains to smart grid applications [14].

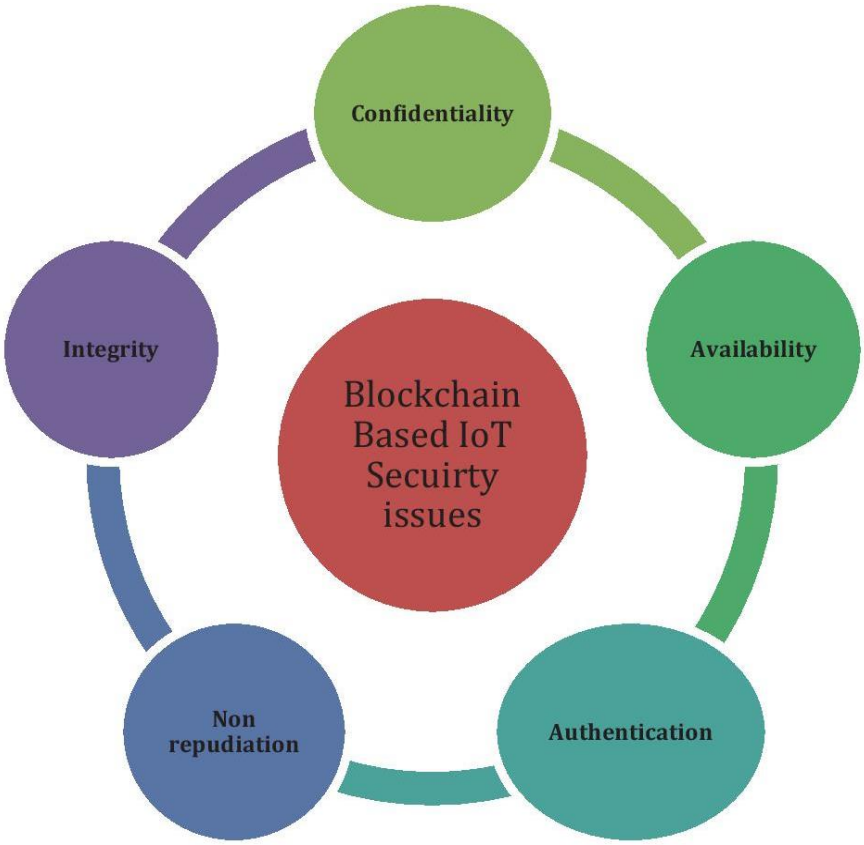

Figure 2: Blockchain based IoT security issues.

Another obstacle that digital forensics must overcome is authentication; individuals who are authorised to handle the evidence must be identified. Blockchain technology is one of the most current options that has been developed to help Internet of Things forensics. Data integrity, immutability, scalability, and security are guaranteed by utilising Blockchain technology in digital forensics. Consequently, this article's goal is to give a thorough evaluation of IoT forensics and security, with a focus on the potential integration of Blockchain technology. It starts with an extensive introduction to Blockchain and Internet of Things (IoT) security which is shown in figure 2, before moving on to discuss the importance of IoT forensics and the basics of the IoT. The next section discusses the difficulties of using blockchain technology for forensics and Internet of Things security. The paper concludes with a discussion of potential future study directions.

As part of our research, we build a V&V process model for cyber security control to fix the problem. Based on the idea of adaptive focused testing, this model was developed. Along with this, a quantitative method is created to identify and prioritise the information security measures that are most prone to errors. The built model may provide an additional and more reliable basis for the subjective assessment of experts, according to some evidence [15].

This article delves into the importance of different cyber defence standards and how cyber security frameworks are designed. Security risks, assaults, and ways to safeguard users from cybercriminals are covered in detail. We

next move on to discuss the many issues surrounding cyber security standards. Also covered are the various government initiatives aimed at bolstering cyber defences, as well as the national information security policy's stated goal of doing just that. At long last, we have some serious guidelines for keeping data secure and protected [16]. Read on to learn about the criteria that the federal government uses to assess the HHS's cybersecurity practices.

In order for cybersecurity policies and procedures to safeguard the operational resources and objectives of the US Department of Health and Human Resources, they must be in line with existing federal regulations and standards. Furthermore, we aim to promote security best practices for protecting information systems from cyber threats and unauthorised individuals [17]. As a bonus to making order fulfilment more efficient, this automation helps cut down on human error in the processing of orders. However, that could be disrupted by cyberattacks, particularly those that originate from the Internet. In order to counter a threat to the quantum response (QR), this research proposes a novel attacker-defender model. This model's goal is to safeguard critical assets by considering the defensive budget and relying on features simultaneously. In terms of the solution, the desirability of protecting any asset is indicated by its level of protection [18]. This article provides an overview of deep learning algorithms that can detect cyber security attacks and compares the datasets used for the research.

For the purpose of this article, we will focus on intrusion detection systems that use deep learning techniques. We identify 35 popular cyber datasets and group them into seven types because of the key role the dataset plays in intrusion detection: Examples of datasets that fall under this category include electric network, internet, virtual private network, android device, internet of things, and internet link datasets [19].

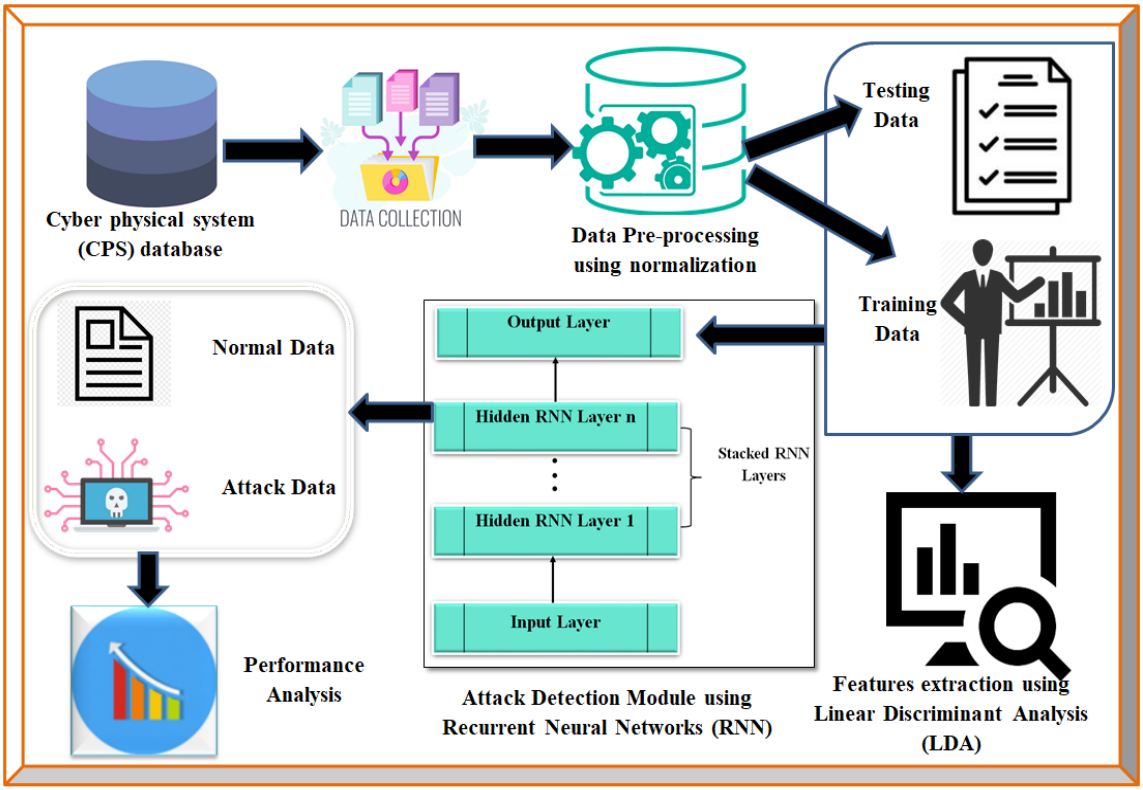

Figure 3: A Strong Framework for Cyber Attack Detection Based on Deep Learning

The security of local and satellite networks is increasingly being threatened by criminal activity and attempts to penetrate them. In order to ensure the safety of online resources, it has been determined that the strategies and methods for intrusion detection are absolutely necessary. With more and more gadgets linking to the internet, cyber security is becoming more and more important.

When there is an intrusion, there are several things that are violated, including security principles like as integrity and confidentiality. For the purpose of attacking a network and searching for vulnerabilities, the adversary makes use of technologically advanced programming tools. In light of this, the intrusion detection strategy is an essential component for monitoring and preventing intrusions in the environment of a computing network.

To automatically identify and categorise intrusions at network and host rates, intrusion detection systems (IDS) often employ techniques from machine learning. These systems aim to detect and categorise cyberattacks in a

timely way. Conversely, a plethora of difficulties emerge when malicious assaults are dynamic and occur in massive quantities, calling for a scalable solution. For the benefit of future studies in the field of information security, the public has access to a plethora of malware databases [20].

By utilising deep learning approaches, this research aims to efficiently and automatically create feature representations that are relevant to large amounts of unlabeled raw network traffic data. Automated learning approaches will be used to achieve this. By combining stacked dilated convolutional auto encoders, we introduce a new network intrusion model and evaluate it on two fresh intrusion detection datasets. This model also includes a novel intrusion detection algorithm. [21] There have been a number of research conducted to see whether or not our strategy will be successful.

Offline network intrusion detection systems (NIDSs) based on deep learning are the focus of this paper's investigation. Making use of a plethora of state-of-the-art deep learning models, we build the detection engine and subsequently assess it quantitatively and comparatively. Our discussion will begin with a general overview of deep learning's approach and its theoretical implications for the network intrusion detection problem. Several machine learning methods will be considered for two distinct network intrusion detection tasks in the following stage [22].

Since the advent of the internet and other technical innovations, there have been profound shifts in human life, social connections, and the natural world. Thanks to wireless technology, a plethora of computers may be attached anywhere, allowing for casual engagement, cooperation, and data access [23]. Recently, CPSs that are complex, cognitive, and possess a high level of self-awareness have been observed. Robots, transport networks, healthcare facilities, smart grids for electricity production, and manufacturing 4.0 for the manufacturing sector are all part of this [24]. Reasons for this include the complex interplay between many cyber and physical components and the high likelihood of unexpected occurrences causing significant disruptions to CPS activity.

When it comes to CPS activity, it is difficult to make accurate predictions. Meanwhile, researchers in both the commercial world and the academic world are concentrating their efforts on cyber security for CPS. This is due to the increasing frequency and level of sophistication of assaults, which are also referred to as zero-day vulnerabilities [25]. This is the fundamental structure of the CPS, as seen in Figure 4.

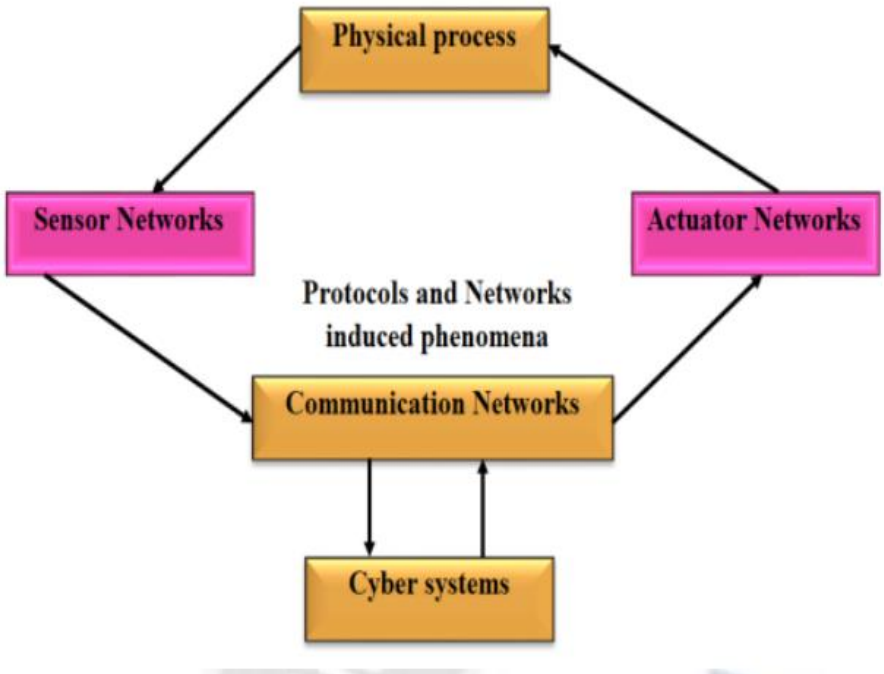

Figure 4: Basic CPS structure

In addition to the assistance of security professionals, it is necessary to collaborate across a variety of AI and ML technologies in order to prevent malicious attacks that exploit zero-day vulnerabilities [26]. Due to the fact that human-machine collaboration strives to reduce the number of instances in which false convictions are made, human decision-making makes detection systems more effective. As a result of the fact that cyberattacks have the potential to interfere with the routine execution of physical procedures on CPS, traditional machine learning algorithms are utilised in order to identify them. When networks are complicated, it becomes difficult to conduct a

definitive assessment of cyberattacks against CPS. Additionally, there is a need for greater expertise regarding the subject matter that is being investigated. Neural networks have the potential to be greatly improved in terms of their capabilities and efficiency with the use of artificial intelligence concepts and techniques. Given that it is composed of several layers, the neural network has the potential to surprise with traits that are not immediately obvious and then progress to more complex ones.

Conclusion

The purpose of this research was to determine which cryptographic algorithm is the most effective for a certain field of application by conducting an in-depth analysis of a number of different algorithms. The following variables are utilised in order to evaluate the performance of cryptographic algorithms: Security, protection from attacks, encryption ratio, speed, key-length, and tunability. Image processing makes use of DES, smart cards and online payments of 3DES, and database security and online shopping of Blowfish. According to our research, AES is a good fit for both wireless communication and financial institutions. While RSA is great for online banking, DSA is more suited to web apps and email verification, and ECC is the way to go for key exchange in web and mobile apps. Conversely, DSA works well for email verification as well. A total accuracy of 97.321% in classifying users into specific groups was achieved by the proposed framework, making it the clear winner. Traditional models like ResNet-50, Deep Neural Network (DNN), Multi-layer Perceptron (MLP), and Self-Organizing Incremental Neural Network (SOINN) failed miserably when it came to making accurate predictions.The technical system's sensors will use the methods outlined in this study to collect all the fresh data. Some other methods for coming up with ideas will then be compared to it.

After the researchers have finished developing a reliable prediction model, they will then build strategies for maintaining safety in environments that could potentially be harmful.

References

[1]. Sakala, L., & Phiri, J. (2019). Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model. Open Journal of Business and Management, 7, 1380-1394. https://doi.org/10.4236/ojbm.2019.73095

[2]. Nawaz, M., Motiwalla, L., & Deokar, A. V. (2018). Usage-Driven Personalised Mobile Banking Application: A Research Prototype. In The Proceedings of the 2018 ACM SIGMIS Conference on Computers and People Research (p. 159). Association for Computing Machinery. https://doi.org/10.1145/3209626.3209736

[3]. Sethi, D., & Acharya, D. (2018). Financial Inclusion and Economic Growth Linkage; Some Cross-Country Evidence. Journal of Financial Economic Policy, 10, 369-385. https://doi.org/10.1108/JFEP-11-2016-0073

[4]. Purohit, S., & Arora, R. (2021). Adoption of Mobile Banking at the Bottom of the Pyramid: An Emerging Market Perspective. International Journal of Emerging Market, 18, 200-222. https://doi.org/10.1108/IJOEM-07-2020-0821

[5]. McDonald, N. G. (2020). Past, Present and Future Methods of Cryptography and Data Encryption: A Research Review. Master's Thesis, University of Utah.

[6]. Falade, P. V., & Ogundele, G. B. (2022). Vulnerability Analysis of Digital Banks' Mobile Applications. NDA Journal of Military Science and Disciplinary Studies, 1, 44-55.

[7]. Lula, P., Dospinescu, O., Homocianu, D., & Sireteanu, N. A. (2021). An Advanced Analysis of Cloud Computing Concepts Based on the Computer Science Ontology. Computers, Materials & Continua, 66, 2425-2443. https://doi.org/10.32604/cmc.2021.013771

[8]. Joshi, K., Gill, S., & Yadav, R. A. (2018). New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications, 2018, Article ID: 9475142. https://doi.org/10.1155/2018/9475142

[9]. Gopinath V, Bhuvaneswaran RS. Design of ECC based secured cloud storage mechanism for transaction rich applications. Computers, Materials & Continua. 2018;57(2):341-352

[10]. Niyaz Ahamed N, Duraipandian N. Secured data storage using deduplication in cloud computing based on elliptic curve cryptography. Computers, Materials & Continua. 2022;41(1):83-94. DOI: 10.32604/csse.2022.020071

[11]. Rajavarmana R, Vetriselvib T, Devic SS. Hybrid security system over banking transaction maintance by a Meta key. Turkish Journal of Computer and Mathematics Education. 2021;12(7):864-868

[12]. Rehman S, Bajwa NT. Hybrid AES-ECC model for the security of data over cloud storage. Electronics. 2021;10(21):2673. DOI: 10.3390/electronics10212673

[13]. M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," Computers and Security. 2020.

[14]. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., 2018.
[15]. C. Lee, H. Bin Yim, and P. H. Seong, "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept," Ann. Nucl. Energy, 2018.
[16]. J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," Futur. Gener. Comput. Syst., 2019.
[17]. I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" Heliyon, 2019.
[18]. K. F. Cheung and M. G. H. Bell, "Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study," Eur. J. Oper. Res., 2019.
[19]. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," J. Inf. Secur. Appl., 2020.
[20]. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, 2019.
[21]. Y. Yu, J. Long, and Z. Cai, "Network Intrusion Detection through Stacking Dilated Convolutional
[22]. J. Yan, D. Jin, C. W. Lee, and P. Liu, "A Comparative Study of Off-Line Deep Learning Based Network Intrusion Detection," in International Conference on Ubiquitous and Future Networks, ICUFN, 2018.
[23]. W. Duo, M. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 5, pp. 784–800, May 2022.
[24]. C. Kwon and I. Hwang, "Reachability Analysis for Safety Assurance of Cyber-Physical Systems Against Cyber Attacks," IEEE Transactions on Automatic Control, vol. 63, no. 7, pp. 2272–2279, Jul. 2018.
[25]. S. Tepjit, I. Horváth, and Z. Rusák, "The state of framework development for implementing reasoning mechanisms in smart cyber-physical systems: A literature review," Journal of Computational Design and Engineering, vol. 6, no. 4, pp. 527–541, Apr. 2019
[26]. R. Prasad and V. Rohokale, "Artificial Intelligence and Machine Learning in Cyber Security," Cyber Security: The Lifeline of Information and Communication Technology, pp. 231–247, Oct. 2019.