Securing the Future of Banking: An IOT-Based Approach to Enhancing Security in the Financial Sector

Omprakash Dewangan
Department of Computer Science and Information Technology,
Kalinga University, Naya Raipur, CG, India.
omprakash.dewangan@kalingauniversity.ac.in

Abstract

The financial sector has always been a prime target for cybercriminals due to the sensitive nature of financial data. Therefore, security has become a crucial aspect of the banking industry, and the emergence of the Internet of Things (IoT) has brought a new approach to addressing security challenges. IoT refers to the connection of various devices, sensors, and systems, allowing them to communicate with each other and collect data. This technology has found its way into the financial industry, providing innovative solutions to various security challenges. This article presents an overview of IoT-based security in the banking sector. It discusses the importance of security in the financial industry, the basics of IoT, and the applications of IoT in banking security. It also explores the various IoT-based security solutions available to banks and the advantages they offer. Moreover, this article highlights the challenges that banks face in implementing IoT-based security systems and the future trends in this field. The article concludes that IoT-based security solutions can enhance the security of banks and the financial sector as a whole. The advantages of IoT-based security solutions include increased efficiency, real-time monitoring, and automation of security processes. However, the implementation of these solutions requires careful planning, as banks face various challenges such as security breaches, lack of standardization, and the high cost of implementation. Therefore, it is recommended that banks carefully assess their security needs and take a holistic approach to implementing IoT-based security solutions.

Keywords: Banking; Cybersecurity; Future Trends; Internet of Things; Security

DOI: 10.48047/ecb/2023.12.si4.987

Introduction to IoT-Based Security in Banking

The financial sector is one of the most targeted industries for cyber-attacks, which can result in data breaches, financial losses, and reputational damage. Therefore, enhancing security in the financial sector has become an essential requirement. One of the latest technological advancements that have the potential to revolutionize security in the financial sector is the Internet of Things (IoT).

IoT refers to a network of interconnected devices and objects that can communicate with each other and exchange data without human intervention. These devices can be embedded with sensors, software, and other technologies that allow them to collect and transmit data, making them ideal for use in enhancing security in the banking industry. IoT-based security solutions in the banking sector can provide real-time monitoring and threat detection, predictive maintenance, and automation of security processes **[1-**

6]. By implementing IoT-based security solutions, banks can better safeguard their assets and customer data, detect and prevent fraudulent activities, and improve customer trust and satisfaction. IoT-based security solutions in banking can include various applications, such as biometric authentication, smart surveillance systems, blockchain technology, and asset tracking. Biometric authentication can help banks to verify the identity of their customers by using facial recognition or fingerprint scanning.

Smart surveillance systems can use IoT sensors to detect suspicious activities and generate alerts for bank security teams to respond proactively. Blockchain technology can help to ensure the integrity of transactions, while asset tracking can help banks to monitor and secure their physical assets. However, implementing IoT-based security in banking also presents certain challenges. One of the main challenges is the need to ensure the security and privacy of data transmitted between IoT devices.

Another challenge is the cost of implementing and maintaining IoT-based security solutions, which may require significant investment in infrastructure and training. IoT-based security has the potential to revolutionize the way security is implemented in the banking sector. With the increasing need for enhanced security in the financial sector, IoT-based security solutions can help banks to better protect their assets and customer data, detect and prevent fraudulent activities, and improve customer trust and satisfaction. However, careful planning, implementation, and maintenance are crucial to overcome the challenges associated with IoT-based security solutions in the banking industry.

The Importance of Security in the Financial Sector

The financial sector is a critical part of any economy, and the security of this sector is of utmost importance. The financial sector is responsible for safeguarding the assets and financial information of individuals and businesses, and any breach in security can have devastating consequences **[6-8]**. In this article, we will discuss the importance of security in the financial sector and the various reasons why it should be a top priority.

Protection of financial assets and information:

One of the primary reasons why security is critical in the financial sector is to protect financial assets and information. Banks and other financial institutions hold a vast amount of sensitive data, including personal information, financial data, and transactional data. Any unauthorized access to this information can lead to identity theft, fraud, and other financial crimes. Therefore, it is crucial to have strong security measures in place to protect these assets and information from cybercriminals.

Maintain customer trust:

Customers entrust their assets and financial information to banks and other financial institutions, and it is the responsibility of these institutions to maintain their trust. A data breach or any other security incident can lead to a loss of trust in the financial institution, which can result in customers leaving and taking their business elsewhere. Therefore, it is essential to ensure that security measures are in place to protect the customers' assets and information, and maintain their trust in the financial institution.

Compliance with regulations:

The financial sector is heavily regulated, and financial institutions must comply with various regulations to operate. Compliance with regulations is not only a legal requirement but also critical to maintaining the trust of customers, investors, and other stakeholders. Strong security measures are necessary to meet these regulations and to demonstrate the institution's commitment to compliance.

Avoiding financial losses:

Cyber-attacks and other security incidents can result in significant financial losses for financial institutions. These losses can be due to direct financial theft, regulatory fines, legal fees, and reputational damage. Therefore, it is crucial to have strong security measures in place to prevent these incidents from occurring and to mitigate the losses if they do occur.

The financial sector is critical to any economy, and the security of this sector is of utmost importance. The protection of financial assets and information, maintaining customer trust, compliance with regulations, and avoiding financial losses are some of the reasons why security is essential in the financial sector. Financial institutions must invest in strong security measures to ensure the security of their assets and information, comply with regulations, and maintain the trust of their customers and other stakeholders.

Understanding the Internet of Things (IoT)

The Internet of Things (IoT) is a term used to describe the network of interconnected physical devices, vehicles, home appliances, and other objects that are embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. In this article, we will discuss the fundamentals of IoT, its applications, and how it works **[9-20]**. IoT comprises devices that are designed to interact with the physical world and communicate with each other via the internet. These devices are equipped with sensors that can detect changes in their environment and other data points. The data collected by these sensors is then processed and analyzed to generate insights, which can be used to make informed decisions.

One of the main benefits of IoT is its ability to automate tasks and provide real-time data. For instance, in smart homes, IoT-enabled devices like thermostats, lighting systems, and security cameras can be controlled remotely through a mobile application, allowing homeowners to manage their homes' systems even when they are away. IoT has numerous applications in various industries, including healthcare, manufacturing, agriculture, transportation, and retail.

In healthcare, IoT can be used to monitor patient health remotely and alert healthcare providers if any issues arise. In manufacturing, IoT can be used to optimize production processes and reduce downtime. In agriculture, IoT can be used to monitor crop growth and optimize irrigation and fertilization. IoT works by connecting devices to a network, which can be a local network or the internet. These devices collect data through their sensors and transmit the data to the network, where it can be processed and analyzed. The data can be sent to a cloud-based platform, where it can be accessed and analyzed by authorized users. One of the main challenges of IoT is the security of the devices and the data they collect. As these devices are connected to the internet, they are vulnerable to cyber-attacks, which can result in data breaches and other security incidents. Therefore, it is essential to implement strong security measures to protect IoT devices and the data they collect.

IoT is a network of interconnected physical devices that can collect and exchange data. It has numerous applications in various industries, and it works by connecting devices to a network, where data can be processed and analyzed. While IoT presents numerous benefits, security remains a significant challenge, and strong security measures must be implemented to protect IoT devices and the data they collect.

IoT Applications in Banking Security

The internet of things (IoT) has become a critical technology for the financial industry, especially in the area of banking security. The use of IoT applications in banking security has increased in recent years due to the need for enhanced security measures to protect against cyber threats **[6, 20-30]**. In this article, we will discuss some of the most common IoT applications in banking security.

- Biometric authentication: Biometric authentication is a technology that uses unique physical characteristics, such as fingerprints or facial recognition, to identify and verify an individual's identity. Many financial institutions are implementing biometric authentication to enhance security and reduce the risk of fraud. IoT devices such as cameras, sensors, and wearables can be used to capture biometric data, which can then be used to verify an individual's identity.
- IoT-based surveillance: IoT-based surveillance systems can help banks monitor their premises and detect potential security breaches. IoT-enabled cameras and sensors can be used to monitor activity in the bank, and any unusual activity can trigger an alert to security personnel. This can help prevent security incidents before they occur, and also provide evidence in the event of a breach.

- Asset tracking: IoT-enabled asset tracking can help banks monitor and track their valuable assets, such as cash or sensitive data. Asset tracking devices can be placed on these assets, which can then transmit data about their location and status to a central monitoring system. This can help banks identify and respond to any potential security threats to their assets.
- Fraud detection: IoT-based fraud detection systems can help banks identify and prevent fraudulent transactions. IoT devices can monitor transaction data in real-time and analyze it for potential signs of fraud, such as unusual transaction patterns or inconsistencies. This can help banks prevent fraudulent transactions before they occur, and also provide evidence in the event of a fraud investigation.
- Cybersecurity: IoT can also be used to enhance cybersecurity in the banking sector. IoT devices can be used to monitor network traffic and detect potential cyber threats. This can help banks respond to cyber-attacks before they cause damage, and also provide valuable insights into the nature of the attack, which can be used to improve security measures.

IoT applications have become essential in banking security due to the increasing cyber threats facing the financial industry. Biometric authentication, IoT-based surveillance, asset tracking, fraud detection, and cybersecurity are some of the most common IoT applications in banking security. These applications can help banks enhance their security measures, protect their assets and data, and improve their response to potential security threats.

IoT-Based Security Solutions for Banks

The banking industry has long been a target for cybercriminals, who seek to exploit vulnerabilities in the banks' security systems to gain access to sensitive customer data and financial information. With the increasing use of technology in banking, the need for strong security measures has become more pressing than ever before **(**see **Figure 1)**. In recent years, the internet of things (IoT) has emerged as a key technology for enhancing security in the banking sector. In this article, we will discuss some of the IoT-based security solutions that banks can implement to enhance their security measures **[1, 30-33]**.

IoT-based surveillance systems: IoT-based surveillance systems can help banks monitor their premises and detect potential security breaches. IoT-enabled cameras and sensors can be used to monitor activity in the bank, and any unusual activity can trigger an alert to security personnel. This can help prevent security incidents before they occur, and also provide evidence in the event of a breach.

Biometric authentication: Biometric authentication is a technology that uses unique physical characteristics, such as fingerprints or facial recognition, to identify and verify an individual's identity. Many financial institutions are implementing biometric authentication to enhance security and reduce the risk of fraud. IoT devices such as cameras, sensors, and wearables can be used to capture biometric data, which can then be used to verify an individual's identity.

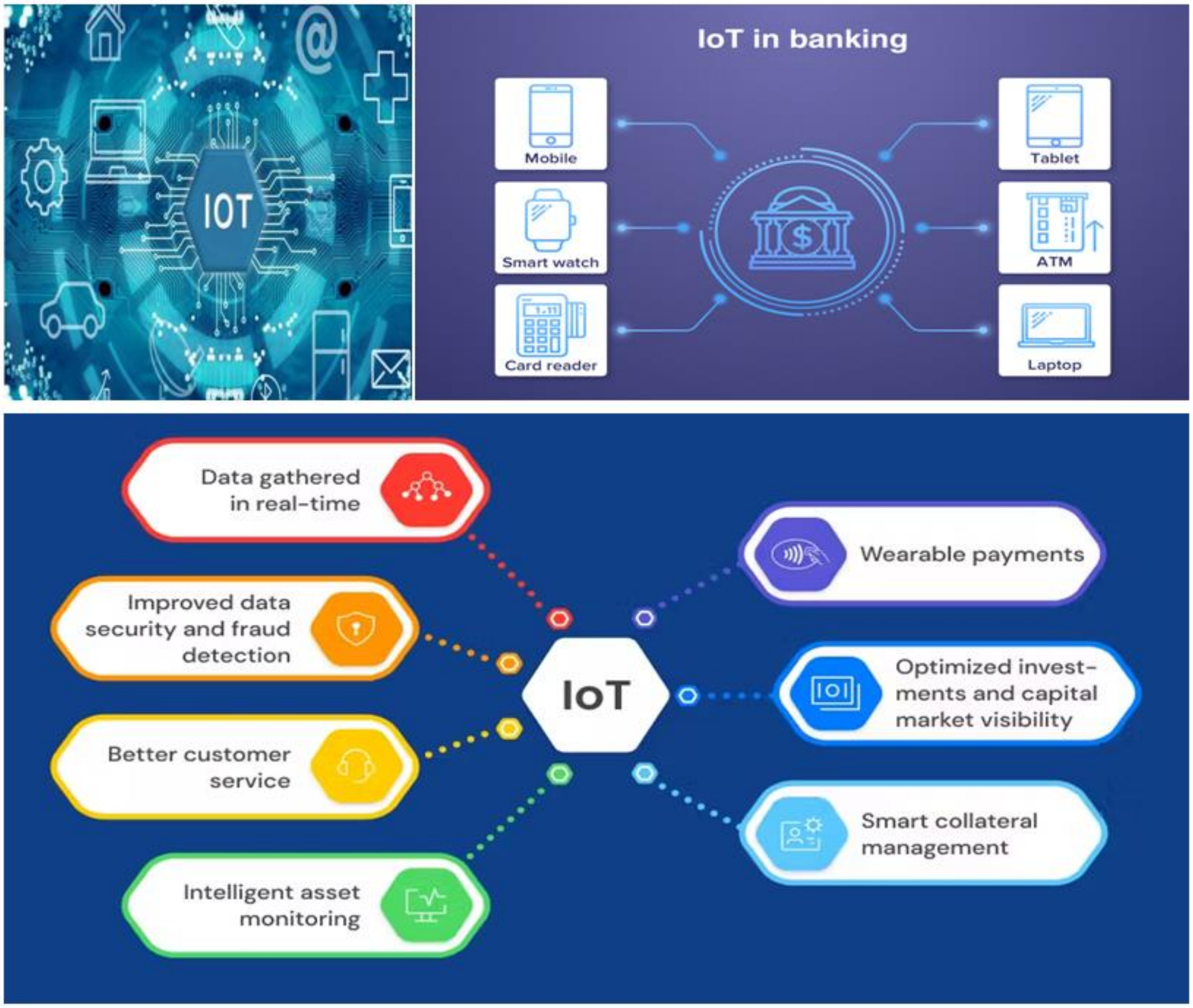
IOT
IoT in banking
Mobile
Smart watch
Card reader
Tablet
ATM
Laptop
Data gathered in real-time
Improved data security and fraud detection
Better customer service
Intelligent asset monitoring
IoT
Wearable payments
Optimized invest-ments and capital market visibility
Smart collateral management

Figure 1. Applied IOT services in banking sector

Asset tracking: IoT-enabled asset tracking can help banks monitor and track their valuable assets, such as cash or sensitive data. Asset tracking devices can be placed on these assets, which can then transmit data about their location and status to a central monitoring system. This can help banks identify and respond to any potential security threats to their assets.

Fraud detection: IoT-based fraud detection systems can help banks identify and prevent fraudulent transactions. IoT devices can monitor transaction data in real-time and analyze it for potential signs of fraud, such as unusual transaction patterns or inconsistencies. This can help banks prevent fraudulent transactions before they occur, and also provide evidence in the event of a fraud investigation.

Cybersecurity: IoT can also be used to enhance cybersecurity in the banking sector. IoT devices can be used to monitor network traffic and detect potential cyber threats. This can help banks respond to cyber-attacks before they cause damage, and also provide valuable insights into the nature of the attack, which can be used to improve security measures.

IoT-based access control: IoT can be used to control access to sensitive areas within a bank. IoT-enabled sensors can be placed at entry points, and access can be granted or denied based on predetermined criteria, such as biometric data or identification credentials. This can help banks prevent unauthorized access to sensitive areas and reduce the risk of security breaches.

IoT-based security solutions have become essential for banks to enhance their security measures in the face of increasing cyber threats. IoT-based surveillance systems, biometric authentication, asset tracking, fraud detection, cybersecurity, and access control are some of the most common IoT-based security solutions that banks can implement to protect their assets and data. By leveraging IoT technology, banks can improve their security measures, reduce the risk of security breaches, and enhance their customers' trust in their services.

Advantages of IoT-Based Security for Banks

The banking industry is a vital sector in the global economy, responsible for safeguarding the wealth and assets of individuals and businesses. With the increasing use of technology in banking, the need for strong security measures has become more pressing than ever before **(**see **Table 1)**. One such technology that has emerged as a key solution for enhancing security in the banking sector is the Internet of Things (IoT) **[33-40]**. In this article, we will discuss some of the advantages of IoT-based security for banks.

Enhanced security: IoT-based security solutions can help banks enhance their security measures by providing real-time monitoring and response to security threats. IoT-enabled sensors and cameras can detect and alert security personnel to any potential security breaches, enabling them to respond quickly and prevent any damage or loss. IoT-based security solutions can also provide valuable insights into security incidents, which can be used to improve security measures and prevent future breaches.

Table 1. Applications of IOT in financial banking sectors

IoT Application	Description
Smart ATMs	IoT-enabled ATMs that can provide personalized services to customers, such as withdrawing cash without a card, facial recognition for identification, and biometric authentication.
Fraud Detection	IoT sensors can detect unusual activity on customer accounts and transactions, such as large withdrawals or purchases from unusual locations.

Asset Tracking	IoT sensors can track the movement of assets such as cash, gold, and documents, providing real-time visibility of their location and status.
Smart Security	IoT sensors can detect unauthorized access, monitor CCTV cameras, and provide real-time alerts to security personnel in the event of a breach.
Predictive Maintenance	IoT sensors can monitor equipment such as ATMs, servers, and other devices, predicting when maintenance is required and reducing downtime.
Customer Experience	IoT devices such as beacons can provide personalized experiences to customers in branches, such as personalized greetings, wayfinding, and targeted promotions.
Risk Management	IoT devices can collect data from various sources to provide a comprehensive view of the bank's risk exposure, such as market data, weather data, and geopolitical events.
Compliance Monitoring	IoT sensors can monitor compliance with regulations such as GDPR, AML, and KYC, ensuring that the bank meets its legal and ethical obligations.

Improved operational efficiency: IoT-based security solutions can improve operational efficiency by automating tasks such as surveillance and access control. IoT-enabled cameras and sensors can monitor the bank's premises and assets, freeing up security personnel to focus on more critical tasks. IoT-based access control can also reduce the need for physical security personnel, thereby reducing labor costs.

Cost-effective: IoT-based security solutions can be cost-effective compared to traditional security measures. IoT devices such as cameras and sensors are relatively inexpensive and can be easily deployed and integrated into existing security systems. This can save banks a considerable amount of money in terms of installation, maintenance, and staffing costs.

Increased customer trust: IoT-based security solutions can increase customer trust by providing a higher level of security and transparency. Customers are more likely to trust banks that use the latest technology to safeguard their assets and data. IoT-based security solutions such as biometric authentication can also provide customers with a more convenient and secure banking experience.

Scalability: IoT-based security solutions are highly scalable and can be easily adapted to meet the changing needs of banks. Banks can add or remove IoT devices as needed, depending on their security requirements. This can help banks respond quickly to changing security threats and ensure that their security measures remain effective.

Data analytics: IoT-based security solutions can provide valuable insights into security incidents and trends through data analytics. By analyzing data from IoT devices, banks can identify potential security threats, improve security measures, and prevent future breaches. Data analytics can also help banks identify operational inefficiencies and improve their overall security posture.

IoT-based security solutions offer several advantages for banks, including enhanced security, improved operational efficiency, cost-effectiveness, increased customer trust, scalability, and data analytics. As the banking industry continues to evolve, IoT-based security solutions will become increasingly essential for protecting the assets and data of banks and their customers.

Challenges to Implementing IoT-Based Security in Banking

The banking industry has undergone significant transformation over the years, and technology has played a crucial role in this evolution. The Internet of Things (IoT) is one such technology that has emerged as a key solution for enhancing security in the banking sector. However, implementing IoT-based security solutions in banking comes with its own set of challenges. In this article, we will discuss some of the challenges to implementing IoT-based security in banking **[35-42]**.

Data privacy and security: The security of data is of utmost importance in the banking industry, and IoT-based security solutions must be designed with data privacy and security in mind. IoT devices are vulnerable to cyber attacks, and if not properly secured, can lead to data breaches and other security incidents. Banks must ensure that their IoT-based security solutions comply with relevant data privacy and security regulations and standards.

Interoperability: IoT-based security solutions often rely on multiple devices and platforms, and interoperability can be a significant challenge. Different devices may use different communication protocols, and integrating them into a single system can be challenging. Banks must ensure that their IoT-based security solutions are compatible with their existing IT infrastructure and can seamlessly integrate with other systems.

Scalability: IoT-based security solutions must be scalable to meet the changing needs of banks. Banks must ensure that their IoT-based security solutions can be easily expanded or contracted as needed, depending on their security requirements. Scalability is crucial to ensuring that IoT-based security solutions remain effective in the face of evolving security threats.

Maintenance and Support: IoT devices require regular maintenance and support to ensure that they remain functional and secure. Banks must ensure that their IoT-based security solutions are properly maintained and supported to prevent device failures and security incidents. This can require a significant investment in terms of time and resources.

Cost: Implementing IoT-based security solutions can be costly, and banks must carefully consider the return on investment. IoT devices can be relatively inexpensive, but the cost of integrating them into existing security systems and maintaining them can add up over time. Banks must ensure that their IoT-based security solutions are cost-effective and provide measurable benefits.

Implementing IoT-based security solutions in banking comes with its own set of challenges. These challenges include data privacy and security, interoperability, scalability, maintenance and support, and cost. Banks must carefully consider these challenges when implementing IoT-based security solutions to ensure that they are effective, secure, and provide measurable benefits. By addressing these challenges, banks can enhance their security posture and protect the assets and data of their customers.

Future Trends in IoT-Based Security in Banking

The use of the Internet of Things (IoT) in the banking industry has revolutionized the way banks operate and provide services to their customers. IoT-based security solutions have also become a key area of focus for banks to enhance their security posture and protect their assets and data. In this article, we will discuss some of the future trends in IoT-based security in banking **[42-54]**.

Artificial Intelligence (AI) and Machine Learning (ML): AI and ML are being increasingly integrated into IoT-based security solutions to enhance their effectiveness. AI and ML can analyze large amounts of data in real-time, detect anomalies, and identify potential security threats. This can help banks detect and prevent security incidents before they occur.

Blockchain: Blockchain technology is being increasingly used in the banking industry for secure and transparent transactions. Blockchain-based IoT devices can be used to create a secure network for banking transactions, reducing the risk of fraud and improving data security.

Biometric Authentication: Biometric authentication is being increasingly used in the banking industry to enhance security. IoT-based devices such as fingerprint scanners and facial recognition technology can be used to authenticate users and prevent unauthorized access to sensitive data.

Cloud-Based Security: Cloud-based security solutions are becoming increasingly popular in the banking industry. Cloud-based IoT devices can provide enhanced security features such as real-time threat detection, data encryption, and secure access to data from any location.

Quantum Computing: Quantum computing is an emerging technology that has the potential to revolutionize the banking industry. Quantum computing can be used to develop more secure encryption algorithms and enhance security in IoT-based devices.

The use of IoT-based security solutions in the banking industry is expected to grow significantly in the coming years. Future trends in IoT-based security in banking include the integration of AI and ML, the use of blockchain technology, biometric authentication, cloud-based security, and quantum computing. Banks that invest in these technologies are likely to enhance their security posture, improve customer trust, and gain a competitive advantage in the marketplace.

Conclusion and Recommendations for IoT-Based Security Implementation in Banking

The banking industry is rapidly adopting the Internet of Things (IoT) to enhance their security posture and protect their assets and data. IoT-based security solutions have become essential for banks in today's digital age, and their adoption is expected to grow significantly in the coming years. In this article, we have discussed the importance of security in the financial sector, the advantages of IoT-based security, the challenges of implementing IoT-based security in banking, and future trends in IoT-based security. In this section, we will provide some recommendations for implementing IoT-based security solutions in banking.

Conduct a Risk Assessment: Banks must conduct a thorough risk assessment before implementing IoT-based security solutions. This includes identifying potential security threats, assessing the likelihood of these threats occurring, and evaluating the potential impact of these threats. A risk assessment can help banks determine the most effective IoT-based security solutions to implement and prioritize their implementation.

Develop a Security Strategy: Banks must develop a comprehensive security strategy that includes IoT-based security solutions. This strategy should include policies and procedures for managing IoT-based devices, securing data, and detecting and responding to security incidents. Banks must ensure that their security strategy complies with relevant data privacy and security regulations and standards.

Choose the Right IoT Devices: Banks must carefully choose IoT devices that are designed with security in mind. IoT devices should have built-in security features such as encryption, authentication, and access control. Banks must also ensure that IoT devices are compatible with their existing IT infrastructure and can seamlessly integrate with other systems.

Monitor and Maintain IoT Devices: IoT devices require regular monitoring and maintenance to ensure that they remain functional and secure. Banks must establish procedures for monitoring IoT devices for security incidents, detecting anomalies, and responding to security incidents. Banks must also ensure that their IoT-based security solutions are properly maintained and updated to prevent device failures and security incidents.

Invest in Training and Education: Banks must invest in training and education to ensure that their employees are aware of the risks associated with IoT-based security and how to manage them. This includes providing training on IoT-based devices, security procedures, and incident response.

Implementing IoT-based security solutions in banking requires careful planning, risk assessment, and investment in training and education. Banks must choose the right IoT devices, develop a comprehensive security strategy, monitor and maintain IoT devices, and invest in training and education. By following these recommendations, banks can enhance their security posture, protect their assets and data, and gain a competitive advantage in the marketplace.

References

[1]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/comst.2015.2444095

[2]. Biswas, S., & Weimerskirch, A. (2020). Internet of Things: A review of applications in banking and financial services. Journal of Financial Services Research, 57(1), 101-120. https://doi.org/10.1007/s10693-019-00324-1

[3]. Chryssanthou, A., & Sgouropoulou, C. (2019). Internet of things (IoT) applications in financial services: A systematic literature review. Journal of Financial Services Marketing, 24(2), 98-111. https://doi.org/10.1057/s41264-018-0067-8

[4]. Gai, K., Qiu, M., & Liu, L. (2019). A comprehensive survey of Internet of Things (IoT) security: Research progress and challenges. IEEE Internet of Things Journal, 6(3), 3876-3894. https://doi.org/10.1109/jiot.2019.2923

[5]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[6]. Han, J., Li, X., Zhang, L., Jiang, B., & Chen, C. (2020). Security and privacy in the Internet of Things: A survey. IEEE Internet of Things Journal, 7(10), 9155-9173. https://doi.org/10.1109/jiot.2020.3007053

[7]. Islam, M. S., Islam, M. M., Hossain, M. S., & Kwak, D. (2015). The Internet of Things for health care: A comprehensive survey. IEEE Access, 3, 678-708. https://doi.org/10.1109/access.2015.2437951

[8]. Miorandi, D., Sicari, S., Pellegrini, F. D., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[9]. Sarma, N., Kotamraju, N., Kumar, R., & Gopalakrishnan, S. (2020). Internet of Things (IoT) and its applications in banking industry. Procedia Computer Science, 171, 67-76. https://doi.org/10.1016/j.procs.2020.03.167

[10]. Xie, J., Zhou, W., & Li, Y. (2020). A survey on IoT-based smart security systems for financial industry. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3497-3509.

[11]. Joshi, A., Roy, S., Manik, R. K., & Sahoo, S. K. (2023). Scientific Philosophy: Exploring Existential, Metaphysical, and Ethical Research Philosophy Behind the Question “WHO AM I?”. Journal of Pharmaceutical Negative Results, 1648-1671.

[12]. Manik, R. K., Dubey, S., & Joshi, A. (2023). The Effect of Possible Yogic Practices in Management of Pregnancy Induced Hypertension. Journal of Survey in Fisheries Sciences, 10(1S), 4237-4246.

[13]. Manik, R. K., Jain, D., & Joshi, A. (2023). Effect of Naturopathy and Ayurveda on Cystic Fibrosis: Detailed Review analysis. Journal of Survey in Fisheries Sciences, 10(1S), 4214-4230.

[14]. Joshi, A., Manik, R. K., Kumar, P., Roy, S., Jain, D., & Sarkar, P. (2022). Brain Fingerprinting: The New Era of Truth and Lie Detection. Advanced Engineering Science, ISSN, 2096-3246.

[15]. Borkotoky, S., Joshi, A., Kaushik, V., & Jha, A. N. (2022). Machine Learning and Artificial Intelligence in Therapeutics and Drug Development Life Cycle. IntechOpen.

[16]. Joshi, A., Vats, N., Singh, H., & Kaushik, V. (2022). Quercetin Compound Analysis to Develop Treatment for Dementia Associated with Alzheimer? s disease in Humans: In-silico Study. Journal of Drug and Alcohol Research, 11(4), 1-7.

[17]. Joshi, A., Sharma, V., Singh, J., & Kaushik, V. (2022). Chemi-Informatic Approach to Investigate Putative Pharmacoactive Agents of Plant Origin to Eradicate COVID-19. Coronaviruses, 3(3), 40-54.

[18]. Sunil Krishnan, G., Joshi, A., & Kaushik, V. (2021). Bioinformatics in personalized medicine. Advances in Bioinformatics, 303-315.

[19]. Joshi, A., & Kaushik, V. (2021). Big Data and Its Analytics in Agriculture. Bioinformatics for agriculture: High-throughput approaches, 71-83.

[20]. Joshi, A., Solanki, D. S., Gehlot, P., Singh, J., & Kaushik, V. (2022). In-Silico Validation of Prosopis ciniraria Therapeutic Peptides Against Fungal Cell Wall: Better Treatment Strategy for Fungal Diseases. International Journal of Peptide Research and Therapeutics, 28, 1-9.

[21]. Vats, N. E. H. A., Joshi, A. M. I. T., Kour, S. A. R. A. N. J. E. E. T., & Kaushik, V. I. K. A. S. (2021). Covid-19 pandemic: pathological, socioeconomical and psychological impact on life, and possibilities of treatment. International Journal of Pharmaceutical Research, 2724-2738.

[22]. Krishnan, S., Joshi, A., & Kaushik, V. (2021). The Differentially Expressed Genes and Biomarker Identification for Dengue Disease Using Transcriptome Data Analysis. Journal of Drug and Alcohol Research, 10(6).

[23]. Joshi, A., Ray, N. M., Badhwar, R., Lahiri, T., & Kaushik, V. (2020). Application Of Hmm-Viterbi Model For Identification Of Epitopic Signature Within Screened Protein-Antigens Of Hepatitis C Virus. European Journal of Molecular & Clinical Medicine, 7(07), 2020.

[24]. Sarkar, P., & Joshi, A. (2023). Applied Mathematical Modelling in Evolutionary Biochemistry. Scandinavian Journal of Information Systems, 35(1), 68-75.

[25]. Sarkar, P., & Joshi, A. (2023). Applications of Cauchy’s Integral Theorem in Analysing Cell Division. Journal of Clinical Otorhinolaryngology, Head, and Neck Surgery, 27(1).

[26]. Sarkar, P., & Joshi, A. (2023). An Engineering Perspective on the Biomechanics and Bioelectricity of Fishes. Journal of Survey in Fisheries Sciences, 10(4S), 2201-2219.

[27]. Joshi, A., Sasumana, J., Ray, N. M., & Kaushik, V. (2021). Neural network analysis. Advances in Bioinformatics, 351-364.

[28]. Saxena, R., Joshi, A., Joshi, S., Borkotoky, S., Singh, K., Rai, P. K., ... & Sharma, R. (2023). The role of artificial intelligence strategies to mitigate abiotic stress and climate change in crop production. In Visualization Techniques for Climate Change with Machine Learning and Artificial Intelligence (pp. 273-293). Elsevier.

[29]. Rai, P. K., Joshi, A., Abraham, G., Saxena, R., Borkotoky, S., Yadav, R. K., ... & Tripathi, K. (2022). Cyanobacteria as a Source of Novel Bioactive Compounds. Role of Microbes in Industrial Products and Processes, 145-170.

[30]. Joshi, A., Joshi, B. C., Mannan, M. A. U., & Kaushik, V. (2020). Epitope based vaccine prediction for SARS-COV-2 by deploying immuno-informatics approach. Informatics in medicine unlocked, 19, 100338.

[31]. Joshi, A., Pathak, D. C., Mannan, M. A. U., & Kaushik, V. (2021). In-silico designing of epitope-based vaccine against the seven banded grouper nervous necrosis virus affecting fish species. Network Modeling Analysis in Health Informatics and Bioinformatics, 10(1), 37.

[32]. Kaushik, V., Jain, P., Akhtar, N., Joshi, A., Gupta, L. R., Grewal, R. K., ... & Chawla, M. (2022). Immunoinformatics-aided design and in vivo validation of a peptide-based multiepitope vaccine targeting canine circovirus. ACS Pharmacology & Translational Science, 5(8), 679-691.

[33]. Joshi, A., Ray, N. M., Singh, J., Upadhyay, A. K., & Kaushik, V. (2022). T-cell epitope-based vaccine designing against Orthohantavirus: a causative agent of deadly cardio-pulmonary disease. Network Modeling Analysis in Health Informatics and Bioinformatics, 11, 1-10.

[34]. Joshi, A., Krishnan, S., & Kaushik, V. (2022). Codon usage studies and epitope-based peptide vaccine prediction against Tropheryma whipplei. Journal of Genetic Engineering and Biotechnology, 20(1), 41.

[35]. Joshi, A., Kaushik, V., & Singh, J. (2019). Comparative Analysis of Genomic Data To Determine Codon Usage and Amino Acid Usage in Tropheryma Whipplei. Think India Journal, 22(16), 67-78.

[36]. Agarwal, R., & Nair, R. R. (2018). Internet of Things (IoT) for financial services: A systematic literature review. Journal of Advances in Management Research, 15(2), 162-178. https://doi.org/10.1108/jamr-07-2017-0045

[37]. Arpaci, I. I., & Gokmenoglu, E. A. (2021). Internet of Things (IoT) based security and privacy solutions for the banking industry: A comprehensive review. Journal of King Saud University-Computer and Information Sciences, 33(3), 356-374. https://doi.org/10.1016/j.jksuci.2020.09.014

[38]. Bhushan, B., & Bhatia, V. (2020). Internet of Things (IoT) and security challenges: A comprehensive review. Computers & Security, 92, 101743. https://doi.org/10.1016/j.cose.2020.101743

[39]. Goyal, S., & Bhatnagar, S. (2017). Internet of Things (IoT): A review of applications in healthcare. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(2), 624-630.

[40]. Huang, X., Li, S., Xiao, Y., Li, Y., & Li, Y. (2020). Research on IoT application in banking industry: Taking smart bank as an example. Mobile Networks and Applications, 25(4), 1341-1348. https://doi.org/10.1007/s11036-019-01264-5

[41]. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

[42]. Li, Z., Chen, M., & Chen, J. (2020). Edge computing for the internet of things: A survey. IEEE Internet of Things Journal, 7(11), 10377-10407. https://doi.org/10.1109/jiot.2020.3008585

[43]. Liu, Y., Lu, R., & Yang, X. (2017). Blockchain and Internet of Things-based security framework for healthcare industry. Journal of Medical Systems, 41(8), 129. https://doi.org/10.1007/s10916-017-0776-1

[44]. Mishra, P., Kumar, P., & Mishra, R. (2019). An internet of things (IoT) based security framework for smart banking. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1094-1098). IEEE. https://doi.org/10.1109/iccmc.2019.8867865

[45]. Yang, F., Li, X., & Li, C. (2019). IoT-based home automation system: Overview and security issues. International Journal of Distributed Sensor Networks, 15(11), 1550147719883869.

[46]. Sarkar, P., & Dewangan, O.. (2022). Applying Advanced Deep Learning to Optimize Clinical Image Analysis. NeuroQuantology, 20(21), 123–129.

[47]. Dewangan, O., & Sarkar, P. (2022). A Study on Network Security Using Deep Learning Methods. Advanced Engineering Science, 54(02), 6393 – 6404.

[48]. Sarkar, P., & Dewangan, O.. (2023). Augmented Reality-Based Virtual Smartphone. Journal of Data Acquisition and Processing, 38(2), 1983–1990.

[49]. Sarkar, P., & Joshi, A. (2023). An Explorative Review on Fishes Biomechanics and Bioelectricity. Acta Biomedica, 94(1), 281-297.

[50]. Sahu, S., & Dewangan, O. (2015). Enhanced Log Cleaner with User and Session based Clustering for Effective Log Analysis. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 4(6), 2610-2615.

[51]. Dansena, M. P., & Dewangan, M. O. (2015). Adaptive Threshoding for Wavelet Denoising on Medical Images through PSO Algorithm. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 4(5).

[52]. Proshanta Sarkar, Omprakash Dewangan, Amit Joshi*. (2023). A Review on Applications of Artificial Intelligence on Bionic Eye Designing and Functioning. Scandinavian Journal of Information Systems, 35(1), 1119–1127.

[53]. Omprakash Dewangan & Dr. Megha Mishra. (2022). An Implementation of Sentiment Analysis with Multiple Modalities using a Machine Learning. Harbin Gongye Daxue Xuebao/Journal of Harbin Institute of Technology, 54(8), 378–386.

[54]. Dewangan, O., & Mishra, M. (2021). An Approach of Multimodal Sentiment Analysis using Machine Learning. Webology, 18(6), 8491–8503.