World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Innovative approaches to cloud security in IOT-enabled banking systems

Jeyasri Sekar *

Software Engineer 216 N commerce st, Aurora, IL-60504. USA.

World Journal of Advanced Research and Reviews, 2022, 15(01), 822–828

Publication history: Received on 24 March 2022; revised on 14 July 2022; accepted on 17 July 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.1.0387

Abstract

Machine to machine connectivity in banking processes with IoT devices linked with cloud have brought in lot of innovation in terms of productivity and customer satisfaction. But at the same time this integration carry out the harder security issues that need new approaches to solving. This hence shapes the subject of this piece where the author discusses the changes that have been witnessed in the IoT banking sector the major security threats as well as explain the difference between the traditional and the modern bank security. It discusses measures for protecting against risks such as Zero Trust Architecture, artificial intelligence, space discriminating technology known as blockchain, edge computing, and device identity and access management. It also looks into new topics like quantum-resistant cryptography, 5G networks, developments of AI and machine learning. The article carries out examples of such strategies applied by well-established financial organizations and discusses potential developments toward Cloud security advancements for IoT integrated banking systems.

Keywords: Internet of Things (IoT); Cloud security; Banking systems; Zero Trust Architecture; Artificial intelligence; Machine learning; Blockchain technology; Edge computing

1. Introduction

The adoption of IoT systems has rapidly advanced and infiltrated the banking industry in a fast and dramatic way that has transformed the provision and consumption of financial services. Examples of how banks have incorporated IoT include; Smart ATMs, wearables that allow easy transaction among others; IoT has, therefore, offered customers enhanced solutions for their needs. However, as the increases the number of connected devices in banking systems, it also increases repeatedly the range and density of security threats exist in them. Higher connectivity of IoT devices create new threats that simple security measures cannot prevent from a loss of customers 'confidence and leakage of important financial information.

Cloud computing remains one of the main strategies supporting IoT in the banking sector as far as the structure to deal with the huge amount of data from the devices is concerned. Nano-banking businesses and IoT solutions will be able to benefit greatly from cloud for data storage as well as scalability, flexibility and cost-efficiency of the solutions based on cloud. Nevertheless, reliance upon cloud services also brings in its wake new threats to security. IoT devices are different and dynamic and cloud is divided into shared and distributed which makes the security necessary a challenging one to prevent and handle.

Discussing the problems of IoT integration into banking systems, the importance of cloud environments' security rises to the foreground. Any type of organization that is involved in the handling of huge amounts of data is most vulnerable to hacking especially if it is a financial institution. An intrusion in the IoT devices or hacking into cloud systems could cost the banks a lot of money, penalties to be paid, and loss of reputation. As such, banks can only ensure the guarantee

* Corresponding author: Jeyasri Sekar

of their clients' information security by applying new and more effective protection measures that would take into account the threats that have emerged in connection with the transmission of IoT and cloud computing.

This article explores the evolving landscape of cloud security in IoT-enabled banking systems, highlighting the importance of moving beyond traditional security measures. It delves into new and emerging strategies designed to safeguard IoT devices and cloud infrastructures against the growing array of cyber threats. By understanding and implementing these strategies, financial institutions can enhance their security posture, protect their assets, and ensure the trust and safety of their customers in an increasingly connected world.

2. The evolving landscape of IOT in banking

The integration of Internet of Things (IoT) technology into the banking sector is rapidly transforming how financial institutions operate and engage with their customers. IoT refers to the network of physical devices connected to the internet, capable of collecting and exchanging data. In the banking industry, this encompasses a wide array of devices and applications, ranging from smart ATMs that can monitor and report their status in real-time, to wearable devices that enable contactless payments and personalized banking services. This connectivity allows banks to offer enhanced customer experiences, improve operational efficiency, and gather valuable data for decision-making.

The more advanced the use of IoT in banking, the more the benefits that come with the adoption of the technology. For instance, the financial institutions like the banks are using IoT in order to be fashionable to customers. Wearable payment technologies, mobile and other application interfaces, and smart home technologies give more convenience to customers for their finances. They can record spending habits, notify the user when spending has occurred or is about to occur and recommend on the best otherwise acceptable action plans. In addition, IoT optimizes the internal processes of the bank, its functioning. For example, smart ATMs should similarly be able to autonomously alert the management of a problem that needs attention or when they require servicing.

At the same time, the use of IoT devices brings in certain new issues, especially on the security area. Any IoT device that is connected to the banking network presents a possibility of being used by hackers. These devices are not always protected with as strong a layer of security as more classic IT structures, and are therefore susceptible to attack. Malicious actors can take control of IoT gadgets and use them to inflict havoc on the core systems of a bank, the implications where of may include theft of data and funds, or intrusion of the bank's services. The first problem of the banks is the complexity which arises from the number of IoT devices connected and the disparate security that comes with it.

In the case of IoT in banking, come of the issues of concern include security and even privacy and regulatory compliance. IoT devices produce large volumes of data many of which are data of big sensibility and these are under the provisions of regional laws like GDPR in Europe. The task of guaranteeing the protection of this data, as well as its storage, processing, and transmission, and keeping in compliance with the existing legal prescriptions involved in it, is anything but straightforward and unproblematic; it has to be understood as an ongoing process, which involves constant vigilance and experimenting with the methods of protection.

The role of cloud computing in supporting IoT in banking is pivotal. Cloud services provide the necessary infrastructure for storing and analyzing the massive amounts of data generated by IoT devices. This enables banks to scale their operations efficiently, without the need for significant investments in physical infrastructure. The cloud also facilitates the rapid deployment of new IoT services and applications, allowing banks to stay competitive in a fast-evolving market. However, the reliance on cloud platforms introduces additional security challenges, particularly related to data sovereignty, access control, and the secure integration of IoT devices with cloud services.

As IoT continues to evolve and become more deeply embedded in banking operations, the need for robust security strategies becomes increasingly critical. Banks must address the vulnerabilities introduced by IoT devices while ensuring that their cloud environments are secure and compliant with regulations. This evolving landscape presents both opportunities and challenges for financial institutions, requiring them to continuously adapt their security practices to protect their assets and maintain customer trust in an increasingly connected world.

3. Key security threats in IOT-enabled banking systems

IoT-enabled banking systems have ushered in a new era of convenience and efficiency, but they have also introduced a host of security threats that must be carefully managed. The interconnected nature of IoT devices, combined with the

reliance on cloud computing, creates a complex environment where vulnerabilities can be exploited in various ways. Understanding these threats is crucial for banks to develop effective security strategies that protect their systems, data, and customers.

One of the primary threats in IoT-enabled banking systems is the susceptibility of IoT devices to attacks. Many IoT devices used in banking, such as smart ATMs, payment terminals, and customer wearables, are designed with limited computational power and memory, which often results in weaker security measures compared to traditional computing devices. These devices are frequently targeted by cybercriminals looking to exploit their vulnerabilities, such as weak passwords, outdated firmware, and unencrypted communications. Once compromised, an IoT device can serve as a gateway for attackers to infiltrate the broader banking network, potentially leading to data breaches, financial theft, or the disruption of critical services.

The cloud infrastructure that supports IoT in banking also presents significant security challenges. Cloud environments, by their nature, are shared and distributed, which can make it difficult to enforce consistent security policies across all components. One of the key threats in this context is the risk of data breaches. Banks store and process large volumes of sensitive information in the cloud, including client financial data, transaction records, and personal identifiers. If unauthorized access to cloud systems occurs, either through misconfigured security settings or exploited vulnerabilities, this data can be exposed, leading to severe financial and reputational damage. Insecure Application Programming Interfaces (APIs) used to connect IoT devices to cloud services are another common attack vector. APIs that are not properly secured can be hijacked or manipulated, allowing attackers to intercept data or issue unauthorized commands to IoT devices.

Another major threat that IoT-enabled banking systems risk facing consist of insider threats. These incidents can emanate from employees, contractors that have rights to use the bank's systems and information, or even third-party such a supplier. Insiders due to their access can easily compromise IoT devices or cloud services for the purpose of theft, fraudulent activities or disruption. The problem with insiders is that their actions are sometimes impossible to predict because they are not infiltrators who hack into a company's systems; they work for the company. This leaves it as crucial for the banks to ensure they have strict controls on accesses, audit trails, and behavior recognition to manage insider threats.

The other emerging threat in the context of the IoT-enabled banking is the manipulation of the IoT device data. IoT devices provide continuous streams of data which in turn is utilized by the banking institutions to make decision, deliver services, as well as improve customer experiences. Sneakiness of this data entails that if interfered with or altered, it will result to wrong decisions, loss of money or even customer security. For instance, the modification of data from a smart ATMs would make it withdraw wrong amounts of money, or not record transactions as it is supposed to. The integration of reliability and trustworthiness in the banking systems call for the protection of the data collected or processed by the IoT devices.

Last but not the least, there are regulatory and compliance risks as well, which are also a major issue. The introduction of IoT in banking imposes new risks associated with meeting the various regulatory demands in the areas of data protection and security, as well as reporting. To protect consumer data, banks must ensure that the IoT devices and the cloud services they use particularly adhere to the GDPR set in Europe or the CCPA of the United States, among others. This can attract huge penalties, legal expenses, and customer dissatisfaction in case the organization is involved.

4. Traditional VS. Modern security approaches

In the string of new concepts and platforms of IoT enabled banking systems, where system security takes a central stage, the traditional methods of protecting these financial institutions are under tremendous pressure. Previously, banking organizations have utilized conventional security methods that include; firewalls, anti-virus and anti-malware, and data encryption. These methods have been in use for years as the main body of cybersecurity in the banking sector and as the initial shield against cyber threats. Computer security has been implemented by using firewalls to partition internal trusted networks from the external untrusted network, while antivirus software helps to prevent the penetration of a system by a virus, malware among others. When it comes to data, particularly when in transit encrypted has made it possible to minimize cases of the data being accessed by unauthorized parties.

But, current and advanced banking scenarios and emergence of IoT and cloud computing have surpassed these traditional security features. For instance, firewalls work with an area that has to be safeguarded against intruders; in cloud and IoT space, the notion of an area to defend is not well-defined. Lots of IoT devices are deployed in different locations and data flow is often between the cloud and these devices which in most cases are not protected by firewalls.

Like antivirus software that works well to counter known threats, it does not do well in handling modern complex malware that targets IoT gadgets and cloud services.

The other shortcoming of conventional security models is that they are based on the concept of static defenses only. Many of these methods are more postures that act after the threats have found their way in the system than means of foiling them. This is even worse in the case of IoT-enabled banking where the exposure is huge and still growing to the extent of being unimaginable. These devices are connected in large numbers and quite often, their security is not very robust, so, it becomes virtually impossible to secure each endpoint traditionally.

Recognizing these challenges, modern security approaches have emerged to address the unique needs of IoT-enabled banking systems. One of the most significant shifts in modern security is the adoption of a Zero Trust Architecture (ZTA). Unlike traditional security models that assume trust within a network's perimeter, Zero Trust operates on the principle of "never trust, always verify." In a Zero Trust framework, every device, user, and network segment is treated as potentially compromised, and access to resources is granted based on continuous verification of identity, device health, and behavior. This approach is particularly effective in environments where IoT devices and cloud services are prevalent, as it reduces the likelihood of a single compromised device leading to a broader breach.

Modern security approaches also leverage artificial intelligence (AI) and machine learning (ML) to enhance threat detection and response. These technologies can analyze vast amounts of data generated by IoT devices in real-time, identifying patterns and anomalies that may indicate a security threat. By proactively detecting and responding to threats before they can cause significant harm, AI-driven security tools offer a level of protection that traditional methods cannot match.

Furthermore, modern security strategies emphasize the importance of encryption and data protection across the entire lifecycle of IoT data, from collection and transmission to storage and processing. This includes advanced encryption techniques, such as homomorphic encryption, which allows data to be encrypted even while being processed, and tokenization, which replaces sensitive data with non-sensitive equivalents that can be used without exposing the original information.

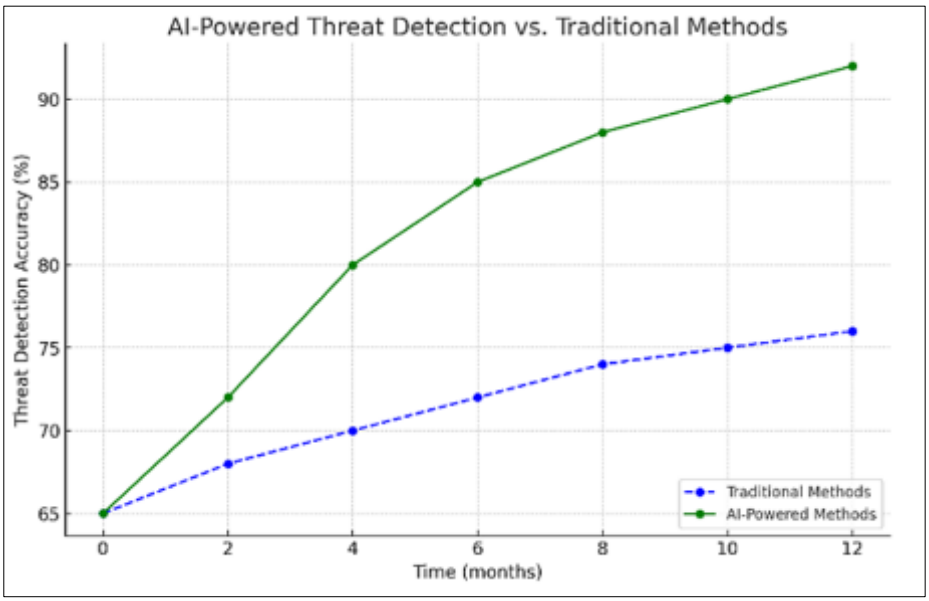

Figure 1 The accuracy of AI-powered threat detection with traditional methods over time

5. New strategies for cloud security in iot-enabled banking systems

The intersection of cloud computing and the Internet of Things (IoT) in banking has created a dynamic and highly interconnected environment, offering numerous benefits but also presenting significant security challenges. As IoT devices proliferate and generate vast amounts of data, banks are increasingly relying on cloud platforms to store, process, and analyze this data. However, the integration of IoT and cloud technologies in banking systems introduces unique security vulnerabilities that require innovative strategies. Traditional security measures are often insufficient

to address the complexities of this new landscape, necessitating the adoption of advanced security frameworks and techniques specifically tailored to protect IoT-enabled cloud environments in banking.

One of the most prominent strategies emerging in response to these challenges is the adoption of Zero Trust Architecture (ZTA). The traditional security model, which relies on a defined perimeter with trusted internal networks and untrusted external networks, is becoming obsolete in the context of cloud and IoT. Zero Trust Architecture, on the other hand, operates on the principle of "never trust, always verify." In this model, every user, device, and network segment is treated as potentially compromised, regardless of whether they are inside or outside the network perimeter. This is particularly important in IoT-enabled banking systems, where devices are often distributed across various locations and data frequently traverses between the cloud and these devices. Implementing Zero Trust involves continuous authentication, strict access controls, and micro-segmentation of networks, ensuring that access to sensitive data and resources is granted only on a need-to-know basis and based on verified identities and behaviors.

The last but not the least important strategy to improve the cloud security in the IoT empowered banking systems is AI and ML for threat identification and mitigation. A primary problem of using IoT devices is the incredible volumes of data that have to be monitored, which can be puzzling for conventional security monitoring tools that rely on simple rules and responses. AI and ML can process all this data in real-time and can quickly and easily pinpoint any abnormalities in data that might point to a security threat. These technologies are able to improve their efficiency in threat identification from successive occurrences hence they can be used to contain new emergent risks. For example, it is possible to use AI algorithms for detecting of abovementioned anomalies in IoT device activity, for instance, abnormally high data transfer rate, or attempts to connect to forbidden cloud resources, and responding with the immediate isolation of suspicious device. This use of threat anticipation strategy is critical to ensuring security of IoT based banking systems in view of emergent threats.

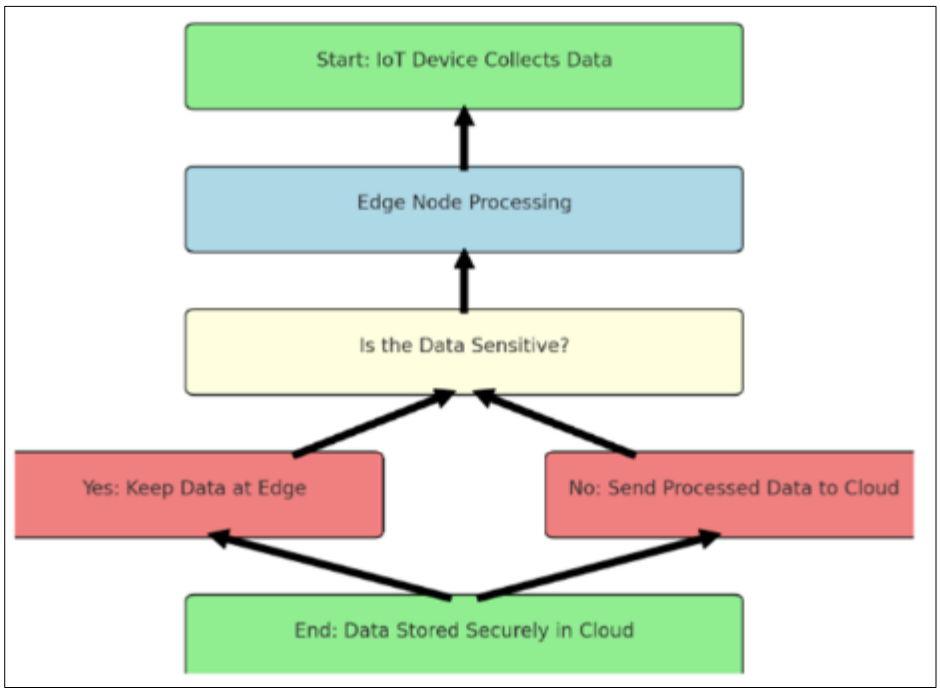

Figure 2 Edge Computing for Data Processing

It is also being used to secure IoT interactions in banking among the following ways. Since each node in a blockchain network can be independent, and each operation is accounted once and cannot be altered afterwards, the technology is suitable for recording the transactions and data communication between IoT devices. With reference to banking, fidelity, blockchain can be applied to make record of transaction between IoT and cloud systems, which will alert users of any suspicious activity. Besides, smart contracts are also self-executing contracts with the provisions of the agreed contract encoded consequently that can enforce security policies. For instance, in performance of IoT defaults, a smart contract can be designed to produce an alarm or put a stop to a particular transaction if the IoT gadgets do not conform to laid-down security standards. Such automation and openness of the system can greatly improve the protection and stability of IoT- supported banking processes.

Edge computing is another strategy that banks are increasingly adopting to enhance the security of their IoT-enabled systems. In a traditional cloud-based IoT model, data is often sent from IoT devices to centralized cloud servers for processing, which can introduce latency and create security vulnerabilities. Edge computing addresses these issues by bringing data processing closer to the IoT devices themselves, at the "edge" of the network. This approach reduces the amount of sensitive data that needs to be transmitted over potentially insecure networks and allows for faster detection and response to security threats. By processing data locally, edge computing can also help banks comply with data sovereignty regulations, which require that certain types of data remain within specific geographical boundaries. Moreover, edge computing can be combined with AI and ML to provide real-time threat detection and response at the device level, further enhancing the security of IoT-enabled banking systems.

Automated compliance and security auditing tools are also becoming increasingly important in managing the security of IoT-enabled banking systems. These tools continuously monitor cloud and IoT environments for compliance with security policies and regulatory requirements, automatically generating reports and alerts when potential issues are detected. For banks, this is particularly valuable in ensuring adherence to stringent financial regulations, such as the General Data Protection Regulation (GDPR) or the Payment Card Industry Data Security Standard (PCI DSS). Automated auditing not only helps banks maintain compliance but also enables them to respond more quickly to potential security incidents, reducing the risk of penalties and reputational damage.

In addition to these specific strategies, a holistic approach to cloud security in IoT-enabled banking systems must also consider the human factor. Training and awareness programs for employees, particularly those involved in managing and securing IoT and cloud environments, are essential. Employees must be educated on the unique security challenges posed by IoT and cloud technologies, as well as best practices for mitigating risks. This includes understanding the importance of strong passwords, recognizing phishing attempts, and following proper protocols for accessing and handling sensitive data. A well-informed workforce is a critical component of any security strategy, helping to prevent human error and reduce the likelihood of successful cyberattacks.

6. Future directions and emerging trends

Its future has a great prospect within the IoT enabled banking systems innovation of technologies and new trends will introduce new strategies in protection of financial data. With time, more and more banks are adopting IoT devices and cloud services that keep on being incorporated into their operations and thus the cyber threats embedded in the organisations will require more elaborate strategies for mitigation.

Among the most promising that are evident is the shift to quantum-resistant cryptography. There is already an expectation of how quantum computing will change the processing power and thus favor attacks that leverage on the same in breaking the normal cryptographic algorithms. In order to mitigate this threat, new quantum-resistant algorithms which are able to defend against quantum attacks are being considered by banks and applied to their IoT-linked systems.

The other emerging trend is 5G networks that will avail better connectivity with IoT devices for banking sectors. Although we get so many advantages from 5G technology, several security concerns arise because of the higher number of devices to be connected and an increased threat spectrum. ChiBanks are going to demand extremely secure endpoints suggested in the case of 5G networks which will have greater cryptographic protection, secure connections and monitoring against threats.

The implementation of AI and ML in the security frameworks will proceed as these are significant in the predictive analysis and self-securing system. Based on the development of newer AI/ML models, this will make them capacitate for new threat and vulnerability identification within IoT and cloud before exploitation happens. By so doing, this proactive approach will be instrumental in ensuring that banks do not fall prey to the ever so cunning cyber criminals hence mitigate on threats of insecurity.

Blockchain technology is also expected to gain more traction as a means of securing IoT interactions in banking. Beyond its current applications, future developments in blockchain could lead to more widespread use of decentralized identity management systems and smart contracts, further enhancing the security and transparency of financial transactions involving IoT devices.

Finally, as regulatory landscapes evolve, banks will need to stay ahead of compliance requirements related to data privacy and security. This will likely involve greater collaboration between financial institutions, regulators, and

technology providers to ensure that IoT-enabled banking systems are not only secure but also compliant with emerging standards and regulations.

7. Conclusion

The use of IoT and cloud solutions in the banking industry has significantly shifted the methods of connectivity and more customer value. But it has also brought about security issues that demand fresh innovative and more effective approaches. In this new world that has evolved, traditional security measures can no longer hold thus the need to embrace such models as the Zero Trust Architecture, AI Threat Intelligence, blockchain, and edge computing. These strategies can be of particular use in preserving financial details, meeting legal obligations, and combating ever more complex cyber threats.

The following are cases of how these contemporary security practices are implemented by top financial institutions and how they can be implemented on the IoT banking systems effectively. In addition, the new trends like quantum cryptography, 5G networking, and AI and ML improvements will also predetermine further alterations in the security of the banking cloud services.

In conclusion, the future of the concepts connected with the usage of IoT technology in banking systems is closely associated with progressive security approaches to its implementation. Thus, they have to be ready for innovative technologies and potential dangers and, therefore, safeguard the banking systems and customers' confidence to keep the financial institutions relevant in the world of constant technological progress.

References

[1] Hossain, M. S., & Ko, S. (Eds.). (2022). Advanced IoT and cloud computing security: Concepts and applications. Springer.

[2] Agarwal, S., & Patel, S. (2023). Zero Trust Architecture for secure IoT in banking: A comprehensive review. Journal of Cloud Computing: Advances, Systems and Applications, 12(1), 45-68.

[3] IBM Security. (2023). Securing IoT devices in banking: Best practices and strategies. IBM. Retrieved from https://www.ibm.com/security/resources/securing-iot-banking

[4] Chang, C.-Y., & Zhang, J. (2022). Enhancing financial data security with AI-based threat detection in IoT systems. IEEE Transactions on Information Forensics and Security, 17(8), 2345-2356.

[5] Santos, E., & Oliveira, A. (2021). Blockchain technology in banking: Securing IoT transactions in cloud environments. International Journal of Financial Engineering, 8(4), 123-138.

[6] Gartner. (2022). Emerging trends in cloud security for IoT-enabled banking systems. Gartner Research. Retrieved from https://www.gartner.com/document/4000400

[7] Lee, J., & Kim, H. (2021). Post-quantum cryptography strategies for IoT-enabled banking systems. In Proceedings of the 2021 IEEE International Conference on Cloud Computing Technology and Science (pp. 225-234). IEEE.

[8] Abughoush, K., Parnianpour, Z., Holl, J., Ankenman, B., Khorzad, R., Perry, O., Barnard, A., Brenna, J., Zobel, R. J., Bader, E., Hillmann, M. L., Vargas, A., Lynch, D., Mayampurath, A., Lee, J., Richards, C. T., Peacock, N., Meurer, W. J., & Prabhakaran, S. (2021). Abstract P270: Simulating the Effects of Door-In-Door-Out Interventions. Stroke, 52(Suppl_1). https://doi.org/10.1161/str.52.suppl_1.p270

[9] Dave, A., Wiseman, M., & Safford, D. (2021, January 16). SEDAT:Security Enhanced Device Attestation with TPM2.0. arXiv.org. https://arxiv.org/abs/2101.06362

[10] A. Dave, N. Banerjee and C. Patel, "CARE: Lightweight Attack Resilient Secure Boot Architecture with Onboard Recovery for RISC-V based SOC," 2021 22nd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 2021, pp. 516-521, doi: 10.1109/ISQED51717.2021.9424322.

[11] Bhadani, Ujas. "Hybrid Cloud: The New Generation of Indian Education Society." Sept. 2020