Security Intelligence Enhanced by Blockchain Data Transitions and Effective Handover Authentication

[1]Vincent Arokiam Arul Raja V and [2]Senthamarai C
[1]Department of Computer Science, Government Arts College, Salem, Tamil Nadu, India.
[2]Department of Computer Application, Government Arts College, Salem, Tamil Nadu, India.
[1]visreg.vinphd@gmail.com, [2]senthamaraiksrct@gmail.com

Correspondence should be addressed to Vincent Arokiam Arul Raja V : visreg.vinphd@gmail.com.

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202404035
Received 08 September 2023; Revised from 17 January 2024; Accepted 07 February 2024.
Available online 05 April 2024.

Abstract – The most significant method is intrusion detection, which improves privacy concerns about client authentication and authorization. No matter what is done to enhance security intelligence, vulnerability has also increased in the modern era. The major role is to predict those vulnerabilities and improve security enhancements by using blockchain methods to enhance privacy concerns. In the corporation, banking, or healthcare system, the major issues are data spoofing, cyber security issues, and viruses affecting confidential data or breaking the shield of data protection. Enhance authorization and authentication by connecting the fog cloud and using the blockchain to protect privacy. In the transition of data, attackers may increase their attacks using various forms. Even if the data is transformed, attackers can easily access it and break the confidentiality of the entire massive database. FCBS (Fog Cloud Blockchain Server) will prevent data vulnerability by using FCS (Fog Cloud Server) modalities for data access. It consists of two segments, AuC (Authentication) and AuT (authorization) during the processing of data. BC (blockchain) addresses the data functionality and enhances the FCS security intelligence in two parts. By preventing the vulnerability earlier, no FC (Fog Cloud) data will be affected. To ensure data protection is reliable and accurate by handing over the AuC and AuT.

Keywords – Handover Authentication, Blockchain, Privacy Preserving, Fog Cloud Blockchain Server, Fog Cloud, Authentication, Authorization.

I. INTRODUCTION

The creation of a fog cloud has emerged as a crucial element in blockchain technology security. Fog computing and blockchain techniques can significantly increase security measures' intelligence. Cloud resources disperse data and computing services across a network, enhancing security and reducing latency. Fog clouds seamlessly integrate into blockchain architecture, enabling the system to distribute data more efficiently, process transactions faster, and increase overall reliability. The use of fog clouds represents a breakthrough in blockchain technology, where security threats are constantly evolving, and intelligence is a top priority.

The concept of a fog cloud server, also known as a fog computing platform, is becoming increasingly significant in today's technology-driven world. Essentially, a fog cloud server is a decentralized system that provides localized storage and processing capabilities for internet-connected devices. By bringing computing resources closer to the end user, fog computing can improve latency and reduce bandwidth usage. This innovative technology has the potential to transform a wide range of industries, from healthcare to transportation. As companies look for ways to provide faster, more reliable, and more efficient services, the cloud server is likely to play a key role in the future of computing.

In the complex landscape of data transmission, malicious attackers are becoming increasingly adept at launching attacks through a myriad of methods. Even if sensitive data is converted or encrypted, these attackers possess the ability to easily breach its security measures, thus compromising the confidentiality of vast databases. However, there is a solution on the horizon in the form of FCBS (Fog Cloud Blockchain Server). By leveraging FCS (Fog Cloud Server) modalities, FCBS effectively safeguards against data vulnerability. Fundamental to this advanced system are two crucial segments: AuC (Authentication) and AuT (Authorization), which collectively ensure the integrity and security of data throughout the entire processing journey.

Blockchain technology has revolutionized businesses, especially when it comes to security. Blockchain traceability and verification effectively prevent security threats, such as attacks and data breaches. This is done by providing a transparent, decentralized approach to recording and verifying transactions. With its immutable nature and cryptographic safeguards, this technology offers businesses a secure and efficient way of tracking assets and verifying transactions. This makes it virtually impossible for ambiguous concepts or security threats to slip through the cracks. As a result, blockchain technology is quickly gaining traction among businesses of all sizes.

Cyber threats are becoming increasingly prevalent in the modern transactional era. One way to achieve this is by implementing authentication and authorization processes that validate users' identities and regulate their access privileges. By doing so, organizations can bolster their security intelligence and establish an additional layer of credential security to prevent unauthorized access attempts. This proactive approach to safeguarding critical data can enhance customer trust, improve compliance, and mitigate data breach risks. In essence, authentication and authorization are essential components of any robust security strategy.

II. RELATED WORKS

Blockchain technology is gaining popularity among millennials because of its exceptional suitability for the information age, according to Hassan et al. (2019). Distributed systems have advanced significantly due to IoT technology improvements in many fields. For storing and distributing data and transactions, the blockchain needs a decentralized data management system. It talks about the blockchain idea and key elements that examine potential security assaults. It also offers current remedies as defenses against these assaults. Additionally, it offers ways to improve blockchain security by summarizing key points used to create different blockchain systems and security tools. This is to address security flaws. Last but not least, it analyzes unresolved difficulties about potential research directions for blockchain-IoT systems [1].

Blockchain has been analyzed by Zhang et al. (2020) as a ground-breaking technology that has a significant impact on contemporary society because of its transparency, decentralization, and security features. Blockchain technology received a lot of attention when cryptocurrencies like Bitcoin were first used. Blockchain technology will soon revolutionize how we communicate, live, and conduct business. Academics, businesspeople, and researchers have recently aggressively looked at blockchain as an emerging technology. To give a thorough overview of blockchain technology's progress, architecture, development frameworks, and security issues. This is in contrast to other blockchain surveys that concentrate on its applications, challenges, attributes, or security [2].

According to Wang et al. (2018), several IoT applications have been developed with (5G) technology to improve (QoS) and user experience, including smart transportation, healthcare, and virtual and augmented reality experiences. Low latency, increased system capacity, high data rates, and energy savings are just a few of the distinctive qualities that the 5G-enabled IoT revolution enables. However, this transformation also produces a considerable volume of data, which makes intelligent and efficient data analysis even more necessary. Data security and privacy issues, such as breaches and sensitive data loss, are also made more problematic by data growth [3].

Conventional data analytics and security techniques cannot support 5G-enabled IoT's particular requirements, notably its high throughput and low latency. It suggests a security framework for intelligent 5G-enabled IoT that uses deep learning (DL) for operations, including intelligent data analysis, and blockchain for data security. The framework's four cloud, fog, edge, and user levels are presented for DL and blockchain activities through a hierarchical architecture. To show the framework's viability in real-world settings, it is simulated and examined using a variety of common measurements of latency, accuracy, and security [4].

According to Kong et al. (2018), the report covers research concerns and a tutorial on the performance evaluation of blockchain-based security and privacy solutions for the IoT. The first part of the article summarizes earlier research on blockchain security for IoT networks. The analysis examines seventeen various IoT application types' blockchain-based security and privacy solutions. These include Industry 4.0, Software Defined Networking, Edge Computing, the Internet of Drones, Clouds, Energy, and Vehicles, among others. Additionally, it compares nine characteristics, such as attack model, scalability, compute, storage, communication costs, and latency, between various consensus algorithms. It also categorizes itself into four categories, including BAN logic, game theory, theory analysis, and security. It also categorizes itself into four categories, which are BAN logic, game theory, theory analysis, and security analysis processes. Additionally, security analysis techniques are covered [5].

The Industrial Internet of Things (IIoT) can enable effective control of the physical environment through vast amounts of industrial data, but Liang et al. (2019) found that data security is difficult because of numerous interconnections and access points. Blockchain technology preserves security and privacy for IoT data. Blockchain networks' overall throughput and scalability can be enhanced using sharding technology. However, because of the unequal distribution of malicious nodes, sharding efficacy is still a problem. It suggests a many-objective optimization algorithm based on the dynamic reward and penalty mechanism (MaOEA-DRP) to optimize the shard validation validity model to enhanceblockchain networks' performance. It is possible to create the ideal blockchainsharding strategy. MaOEA-DRP performs better than other cutting-edge many-objective optimization techniques. The simulation results show that sharding throughput and validity may be greatly increased using our suggested algorithm to provide improved security in blockchain-enabled IIoT [6].

The latest breakthrough in secure and decentralized computing comes in the form of blockchain technology, an innovative concept that is rapidly growing in popularity. Gueta et al. (2019) expertly detail blockchain fundamentals, which include its systematic integration of key components such as a chain structure for data verification and storage, distributed consensus algorithms, cryptographic techniques, and automated smart contracts for seamless data programming and operations. The blockchain serves as an all-encompassing solution, providing unparalleled security measures, ensuring unbeatable access control, and transmitting data efficiently and securely [7].

Impressive advancements in healthcare blockchains have been made with groundbreaking research by Zhang et al. (2018), establishing a pioneering method for securely storing healthcare information. This clever innovation also offers a trusted system for healthcare transactions, with decentralization for ultimate privacy protection. While the industry, government, and academic sectors are eager to adopt this technology, data security, and privacy concerns remain at the forefront of discussion. This is when implementing this method into healthcare systems. Cautious measures must be taken in the implementation of blockchain technology in the healthcare sector [8].

Di Wu et.al (2022), have determined a recent breakthrough in addressing the issue of accurate and scalable predictions in the field of Quality-of-Service (QoS) is the latent factor (LF) model. This model has gained recognition for its impressive efficiency. In order to further enhance the accuracy of LF models, this paper presents the data-characteristic-aware latent factor (DCALF) model, which focuses on identifying user and service neighborhoods based on their geographical information. By employing a density peak algorithm, the DCALF model aims to provide highly precise QoS predictions. With this innovative approach, the DCALF model represents a significant advancement in the field of Web Service and QoS analysis [9]

Wenyuan Xu and et.al have determined that in light of the ever-increasing number of Internet of Things (IoT) devices that continuously generate massive amounts of data, concerns regarding data privacy and network costs have been raised regarding the current cloud-centric approach for IoT big data analysis. To address these concerns, this paper proposes a new efficient Federated Learning (FL) framework called FL-PQSU. This framework allows for the learning of a global model by aggregating local updates from multiple devices without compromising the privacy-sensitive data. By implementing FL-PQSU, we aim to mitigate the challenges associated with data privacy and network costs in IoT big data analysis [10]

Lingwei Xu et.al (2022) have established the integration of the global healthcare industry with artificial intelligence has led to the emergence of diverse intelligent healthcare applications. To meet the high throughput demands of these applications, the Internet of Things (IoT) is set to play a crucial role. In this regard, a significantly enhanced convolutional neural network (CNN) model has been devised. The model incorporates a four-layer convolution and a four-branch inception block, enabling it to leverage various convolution kernels within the same layer. Through this innovative approach, the potential for advancements in intelligent healthcare is limitless [11]

Bin Zhao et.al (2021) have improved the Numerous advancements in artificial intelligence have revolutionized the extraction of valuable insights from vast volumes of industrial big data. Nevertheless, it is disheartening that the vital aspect of ensuring privacy often goes unnoticed in many prevailing techniques. To address this critical concern, a groundbreaking solution is the implementation of differential privacy on shared parameters, coupled with the Gaussian mechanism, thereby guaranteeing the utmost preservation of individuals' privacy. By adopting this cutting-edge approach, stringent privacy measures can now be seamlessly integrated into the process of extracting invaluable information from massive industrial data sets, fostering a secure and ethical digital landscape [12]

Chunyi Zhou et.al (2020) have examined that in the realm of data privacy and security, federated learning stands as an invaluable tool. With its ability to seamlessly merge extensive user groups and collaboratively train models, all while evading the uploading of individual data sets, the server attains a remarkable feat: the prevention of collecting sensitive user information. However, it is imperative to go a step further by proposing a privacy-preserving federated learning scheme within the domain of fog computing. By implementing this scheme, not only will data security and model security be assured, but also an unwavering defense against collusion attacks orchestrated by multiple malicious entities will prevail [13]

Hangjun Zhou et.al (2021) have detected the rapid development of information technologies such as the Internet of Things, Big Data, Artificial Intelligence, and Blockchain has had a profound impact on people's consumption behaviors and completely transformed the development model of the financial industry. In response to this changing landscape, financial institutions are adopting innovative approaches to detect and prevent fraud. One of these approaches is leveraging big data analytics, which involves analyzing large-scale historical data using existing rule-based expert systems and traditional machine learning models. Additionally, the implementation of the graph embedding algorithm Node2Vec has proven to be a valuable tool for identifying and combating internet financial fraud [14]

Zhitao Guan and et.al have proposed that the Smart systems such as the smart grid and Internet of Things have emerged as dynamic solutions to tackle pressing contemporary issues. To ensure privacy and security while performing cluster analysis in the smart grid, we introduce IDPC, the ingenious Differentially Private Clustering algorithm rooted in the Infinite Gaussian mixture model (IGMM). Leveraging the power of nonparametric Bayesian methodology combined with differential privacy, IDPC employs the Laplace mechanism. By seamlessly integrating these cutting-edge techniques, IDPC provides a robust and reliable framework for safeguarding sensitive information in an increasingly interconnected world [15]

III. EXPERIMENTAL STUDY ANALYSIS

Law Enforcement Authority (LEA)

The importance of having an authorized legal entity (LEA) capable of identifying malicious vehicles for network audits cannot be overstated. With the power to determine the identity of a hostile vehicle, LEA is the only agency that can effectively assess and mitigate security risks. By deploying a complete blockchain node on LEA, their significant computing and storage resources can contribute registration data to the blockchain. This ensures that all vehicles and registration information are properly managed while keeping malicious vehicles' real identities concealed. In summary, having a trustworthy LEA is crucial for a secure and trustworthy network environment.

Regional Service Manager (RSM)

The LEA has given RSM, in the form of cloud-based servers with powerful computing and storage capacity, the authority to handle car registration, certification, and cancellation. Each of the numerous domains that make up the overall network has an RSM in charge of maintaining the vehicles in that domain. acts as a full node in each RSM Blockchain network, storing data on car cancellation, registration, and authentication.

Fog Server (FS)

The integration of fog servers and blockchain algorithms has opened up an exciting new chapter in network security and data management. The benefits that this combination offers are numerous and far-reaching, including increased transparency, enhanced data security, and increased efficiency in processing transactions. Specifically, this convergence enables fog servers to act as nodes within a blockchain network. This makes it possible to store, send, and verify data decentralized and securely. With these features, businesses and organizations of all sizes can now leverage blockchain technology without extensive technical expertise or costly infrastructure investments.

Fog Implementation in DM

The integration of fog servers into data mining through blockchain serves as a revolutionary approach to enhancing data security and privacy. By leveraging blockchain's decentralized and immutable features, data can be transmitted and processed efficiently and securely. Fog computing in this context further enhances data processing speed and accuracy, allowing organizations to extract valuable insights from large data sets easily. In essence, the combination of a fog server and blockchain provides a powerful solution for data mining. This is set to transform data analytics.

Fog Saver

Data analysis is an important tool used by organizations to manage their operations in today's digital age. However, with the abundance of sensitive information at stake, ensuring banking data confidentiality and integrity is crucial. Enter the fog saver, a revolutionary tool that leverages data mining and blockchain techniques to protect banking data from cyber threats. With its sophisticated data encryption and verification protocols, the fog saver provides a highly secure environment for financial institutions to store and access critical data. By utilizing this cutting-edge technology, banking institutions can operate with confidence while delivering optimal services to their clients.

Experimental Study Implementation

The emergence of blockchain technology has brought new possibilities to data mining but has also created complexities that require a deeper understanding. These complexities include trust issues, inherent in data mining processes. This is further complicated by decentralized ledgers. To navigate the fog of blockchain in data mining, it is imperative to have a clear understanding of the technology and its potential applications. Expertise in blockchain, cryptography, and data analytics is essential to unlocking the full potential of this groundbreaking data mining technology. It consists of five segments to enhance the security intelligence in the banking system. Fig 1 Show in FCBC Modelling.

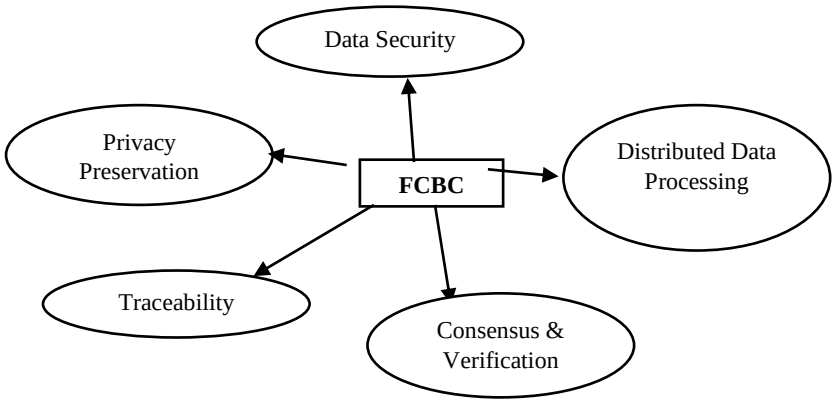


Fig 1. FCBC Modelling

- Data Security: Fog blockchain ensures the security of sensitive data by providing cryptographic mechanisms to protect data integrity and privacy. Immutable and encrypted transactions recorded on the blockchain prevent unauthorized tampering and enhance data security.
- Distributed Data Processing: Fog computing allows for distributed data processing and analysis at the edge of the network. This reduces latency and bandwidth requirements by minimizing data transfers to the cloud. Data mining algorithms can be deployed on fog nodes or edge devices, enabling real-time analysis and insights generation.
- Transparent and Auditable Data Transactions: Fog blockchain maintains a transparent and auditable ledger of data transactions. Each transaction recorded on the blockchain is time-stamped, cryptographically secured, and linked to previous transactions. This transparency enables traceability and accountability in data mining processes.
- Consensus and Verification: Fog blockchain leverages consensus mechanisms, such as proof-of-work (PoW) or proof-of-stake (PoS), to ensure agreement and trust among fog nodes in the network. This consensus process validates data mining results and enhances the reliability of extracted patterns or insights.
- Privacy Preservation: Fog blockchain can provide privacy-preserving mechanisms by allowing participants to retain control over their data. Privacy-enhancing techniques, such as zero-knowledge proofs or differential privacy, can be integrated with Fog blockchain to protect sensitive information during data mining processes.

Modeling Prediction

With a fog blockchain, nodes can be geographically distributed, offering increased redundancy and fault tolerance. In addition, it reduces the cost of maintaining a blockchain network. Furthermore, fog blockchain can improve data transfer and communication efficiency, ensuring blockchain applications remain fast and secure. With blockchain technology, financial institutions must be equipped to navigate a complex and uncertain environment. Fortunately, blockchain offers a myriad of advantages to safeguard user data against unauthorized access and potential breaches. By embracing cutting-edge technology, banks can build trust with their customers and optimize their financial operations with unparalleled accuracy and security. It is essential to partner with experts who navigate the intricate world of blockchain banking.

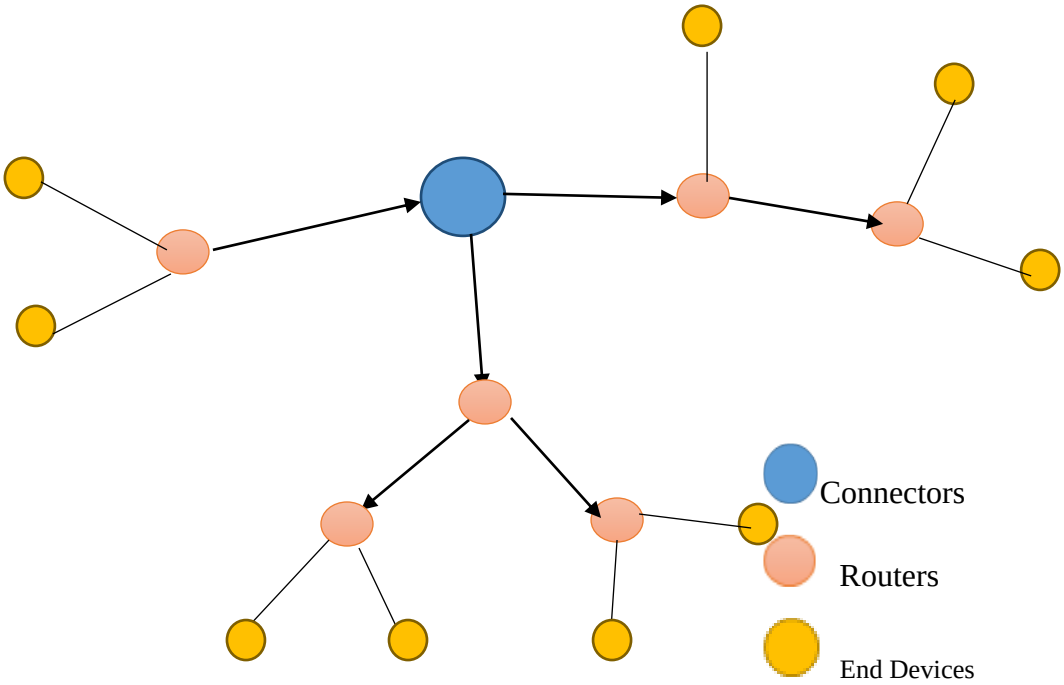


Fig 2. FOG Connections Environment

FOG is used to prevent cyber security issues and enhance banking processing response time. Generally, it faces lots of issues like IP and data spoofing and MitM issues, and security breaches. It is tied to the physical location used to access the data. So attackers can easily attack data and break confidentiality. Utilize blockchain methods to prevent these kinds of issues while accessing online / offline. As shown in **Fig 2**, each router is connected to the connectors and end devices for network communication. To focus on the communication and trace to where it comes from and how to Auc and AuT to the data on the safe side by using the FBC method.

Data mining is a critical process that helps banking professionals identify patterns and insights in vast amounts of information. However, data security is imperative. That's where a cloud-based pairing mechanism comes into play. With its ability to distribute the workload across multiple nodes and encrypt all transferred data, fog blockchain provides a

secure and efficient solution for data mining in the banking sector. By combining this innovative technology with traditional data mining techniques, banks can achieve enhanced accuracy and speed in analysis while safeguarding sensitive information.

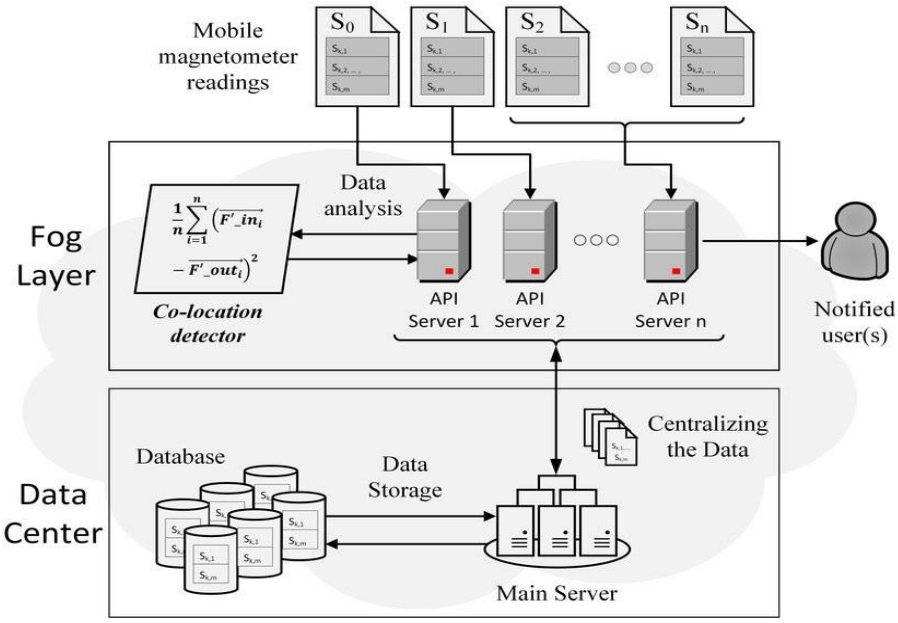


Fig 3. FOGBC Architecture

Fig 3 shows FC close to segmenting the substances that FS in the data accessing platforms. The IEEE 802.15.4 protocol plays a pivotal role in pairing mechanisms designed to safeguard against cyber threats in data mining. By leveraging blockchain technology within a cloud computing environment, this pairing mechanism provides robust security measures that effectively protect sensitive data. The blockchain represents the ideal tool for companies seeking to reduce their vulnerability to cyberattacks due to its sophisticated cryptographic validation system and decentralized storage. By working in tandem with IEEE 802.15.4, blockchain and fog computing are enabling data-driven enterprises to maintain the highest standards of cyber security in an ever-evolving digital landscape.

Fog servers should be deployed from the end node to the end node to ensure efficient and effective data processing since they are located close to the devices and sensors that generate the data in the network. By providing the computational power and networking capabilities needed for processing and storing data on a local device, it facilitates the processing and storing of data. This is before the information is sent to the cloud to be analyzed and stored there. Due to this approach, latency and bandwidth constraints are reduced, making it possible to process data in real time. By offloading the computational burden to the cloud, the Fog Server ensures fast and efficient data processing.

The metrics of jitter and delay detection for fraud detection by analyzing in-time measurement. And the fraud detection and prediction should determine by TTFB for,

$$\text{Delay} = \text{length} / \text{Size of data/bandwidth of network} \tag{1}$$

Depending on the method of time management, the vulnerability might affect the data. By utilizing this BC method, time and AuC can be traced simultaneously. AuC and AuT enable BC to verify a user's identity and trace a function's route in both a preliminary and an end state. FCBC classifies functions into three layers to protect data and enhance security intelligence. The banking system avoids the steps of server down by measuring the delay (Equ 1). AI power management enhances traceability and reveals the client who enters an initial state.

$$\text{Propagation} \propto 1 / \text{Tx speed} \tag{2}$$

Hence the ARM (Association Rule Mining) extract to detect data propagation and transition data to the cloud. Equ 2 determines the speed of transition data and it is related to the substance of FS. There is a possibility that the hardware compliance of the banking system will be affected. So FS can send the backup files from the FC and retrieve them from the same preliminary data without affecting the files. It is necessary to analyze data to enhance security by tracking the three layers of function. Once a step has been completed, the progress can be updated. As this instance is part of a sub-server and controlled by FC, it can be classified as an instance.

$$\text{Tx Speed detection} = \text{distance between x and y} / \text{Tx Speed} \tag{3}$$

Equ 3 reveals the pairing mechanism of the FCB working in data handling and management. Because it is interconnected to the entire end-to-end system. So the distance between interconnected edges is calculated by,

$$= 0.7*3*10^{8}\ m/sec$$
$$= 2.1 * 10^{8}\ m/sec\ (Tx\ speed)$$

To ensure the transition speed of data that is measured by RTT each round. With the ability to aggregate and filter data from multiple devices, conduct local data processing, and transmit only pertinent or condensed information to the cloud, this system offers efficient and effective data management for various applications. Whether it's monitoring energy consumption, tracking assets, or managing medical devices, this technology can streamline processes and enhance accuracy. It does this by sorting through large amounts of data and only sending relevant information to the cloud. The result is a cost-effective and practical solution to managing and analyzing data in realtime.

By leveraging Fog Servers, organizations can enable distributed and localized computing infrastructures, allowing for faster and more efficient data analysis and decision-making. It is particularly useful in scenarios where real-time or low-latency processing is required. Regression is used to determine the problem or co-occurrence analyzed by,

$$P(d) = \log 10 (1+1/d) \quad (4)$$

Where d denotes the leading digit of occurrence in the client entering the banking system. and it is started from 1, 2, 3…… 9 for the data pattern in the problem co-occurrence. To create a cloud server using google cloud and under that, with the help of the development board we are going to create a server called fog server this server is used to reduce the load of the cloud directly the small issues and the minimum number of work is been taken in the control of fog server and the data storage is also being stored in the fog server when it reaches the minimum number of storage it sends to the main cloud.

A unique identifier, an address, and a sum are essential components of security intelligence. The Authentication Center (AuC) plays a vital role in verifying the Authorization Token (AuT) of an end-to-end function and validating whether authentication is valid or not. Furthermore, if a master substance analysis indicates that the correct end-user is not involved, prior messages will notify the end-users and immediately prevent any potential attacks. As such, strict security protocols and vigilant monitoring are essential to safeguard against unauthorized access or intrusion.

$$P(B/A) = P(A\&B) / P(A) \quad (5)$$

Equ 5 is a powerful tool that allows us to calculate the probability of detecting attackers by taking into account the three key parameters previously discussed. By leveraging computational power and potential progress, it can effectively classify the likelihood of an attack occurring. It can also mitigate its impact. This methodical approach enables us to proactively identify and address potential security threats, ultimately safeguarding our systems and preserving operations integrity.

$$(AUB)UC = AU(BUC) \quad (6)$$

Illuminating digital transactions, the system tracks and safeguards against double-spending and tracking attacks. This is done by thoroughly verifying and validating end-user functions. The mathematical representation, displayed as Equ 6, distinctly identifies the finite sets of A, B, and C while data flow control is calculated using probability and consequence. As such, this meticulous process ensures the highest level of security and integrity for financial transactions conducted digitally.

$$Lift = P(T/B) / P(T) \quad (7)$$

$$Lift = P(T\hat{}B) / P(T)\ P(B) \quad (8)$$

Whereas T determines the target and B is a baseline of function. Systems engineering requires T and B to ensure optimal product performance. Analyzing Equ 7 and Equ 8 can predict defect detection and multi-tracking of system functionality. Furthermore, it prioritizes privacy and vulnerability detection to ensure safe and effective functionality. Through careful analysis and consideration of these factors, it provides clients with optimal and reliable results that meet their unique needs and specifications.

Metrics of data confidence level equal to,

$$DI = 100 * (1- Alpha)\ \% \quad (9)$$

The confidence level, represented by alpha equals 0.05 as a result of Equ 9. This is an essential tool to boost data integrity and heighten security intelligence. This valuable metric plays a critical role in determining the reliability of statistical data analysis. It helps to establish statistical parameter boundaries. With a confidence level of 95%, this means that there is only a 5% chance that the results obtained from an analysis test occurred by chance. Therefore, by implementing the results of this equation, one can make informed decisions that significantly impact the overall accuracy and reliability of data analysis.

IV. RESULT AND DISCUSSION

The banking industry faces significant obstacles to preventing and detecting fraudulent activities. In light of this, the industry must adopt creative and cutting-edge technologies to improve security and transparency. This research focuses on an analysis of the use of fog blockchain technology and data mining techniques to enhance fraud detection in bank datasets. As the financial industry evolves, fog computing is becoming increasingly relevant in facilitating complex data analytics and real-time security monitoring. By harnessing the power of these advanced technologies, banks can stay ahead of the game in the constant battle against fraud.

The FCBC is a crucial tool to prevent potential vulnerabilities and enhance security intelligence within the FSB – AuC and AuT systems. Its implementation has significantly heightened data integrity, ensured accuracy, and preserved privacy. This technology has proven to be highly effective at detecting and preventing security breaches, as well as safeguarding sensitive information. With FCBC, the FSB has upheld the highest security standards in its operations. This has protected significant data from spoofing and cyber security issues.

Fig 4. FCB Dashboard

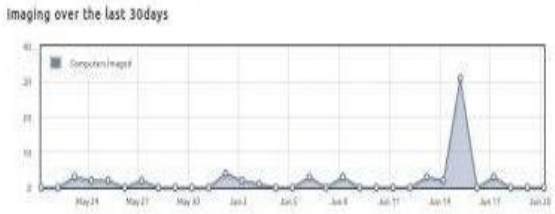


Fig 5. Transition of data

As illustrated in **Fig 4**, the FCBC serves as a crucial vehicle for seamlessly **Fig 5** Show in transitioning data updates and backup sources to the FS. This is necessary to ensure the smooth transmission of up-to-date information. This system is carefully monitored and statistically analyzed daily to enhance privacy-preserving practices. The fundamental importance of this meticulous process lies in its ability to ensure that information is securely stored, updated, and transmitted to prevent unauthorized access. In addition, it retains the confidentiality of sensitive data. It is through these unwavering efforts that the integrity and security of such information is preserved and optimized.

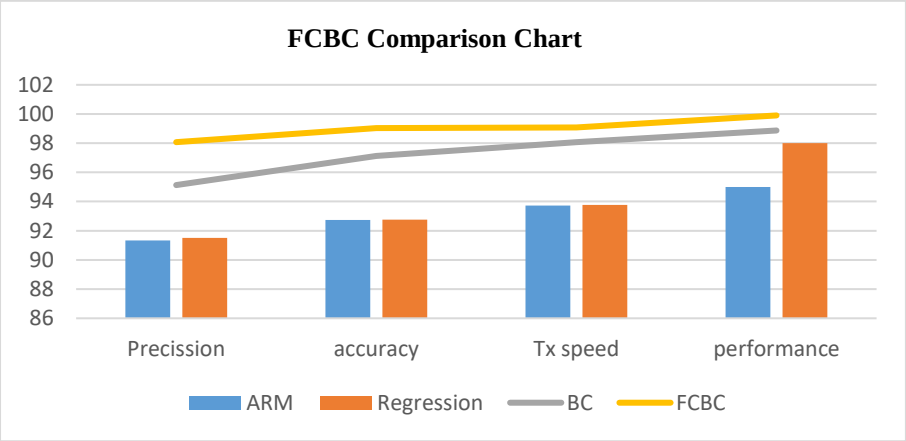
Fig 6. End-User Function

Effective data handling and clear, concise end-user communication are critical to safeguarding against security vulnerabilities and optimizing performance, as demonstrated in **Fig 6** in the FCB report. By implementing robust systems and protocols for handling and storing data, organizations can ensure sensitive information remains secure and protected against unauthorized access. Similarly, by providing clear and user-friendly instructions and interfaces, end-users are empowered to make informed decisions and utilize systems to their fullest potential, leading to improved efficiencies and overall performance. Top-notch data handling and end-user communication are key components of any successful organization.

Table 1 is a valuable resource that demonstrates, with clarity, accuracy, and performance integrity existing and proposed systems. It highlights the significant advantages achieved by implementing FCBC, which has proven to be highly effective in terms of precision. It is integrated with top-of-the-range security intelligence, leading to reinforced security measures. The proposed system has outperformed the existing one, as demonstrated by the striking disparities in

results. These findings show that FCBC technologies are the way forward and can deliver tangible benefits to businesses seeking to enhance data security and accuracy.

Table 1. FCBC Comparison Chart



V. CONCLUSIONS AND FUTURE ENHANCEMENT

Employing the FCBC technique, we have uncovered complex patterns and correlations within our vast dataset, unlocking deeper insights into our data. However, our methods do not stop at analysis. We have integrated the Fog Blockchain, creating an additional layer of security to ensure all transactional processes are verified. Our approach provides a dual benefit- it reduces latency and enhances scalability, while actively serving as a critical aid in detecting and preventing fraud. Our dedication to innovative techniques is evident in our diverse, solution-driven approach to data and security. As data volumes proliferate in every aspect of our lives, data analysis and security become ever more crucial. The future of this field depends on the effective synthesis of cutting-edge tools and artificial intelligence techniques, with the two workings hand-in-hand to better manage and secure the vast amounts of data being generated. From predictive modeling to anomaly detection, the possibilities are almost limitless. Those who harness this combination of technologies effectively will thrive in the data-driven landscape of the future.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References.

[1]. M. U. Hassan, M. H. Rehmani, and J. Chen, “Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions,” Future Generation Computer Systems, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060.

[2]. L. Zhang, Y. Xie, Y. Zheng, W. Xue, X. Zheng, and X. Xu, “The challenges and countermeasures of blockchain in finance and economics,” Systems Research and Behavioral Science, vol. 37, no. 4, pp. 691–698, Jun. 2020, doi: 10.1002/sres.2710.

[3]. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” International Journal of Web and Grid Services, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.095647.

[4]. A. Stranieri, J. Abawajy, A. Kelarev, S. Huda, M. Chowdhury, and H. F. Jelinek, “An approach for Ewing test selection to support the clinical assessment of cardiac autonomic neuropathy,” Artificial Intelligence in Medicine, vol. 58, no. 3, pp. 185–193, Jul. 2013, doi: 10.1016/j.artmed.2013.04.007.

[5]. Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, “Towards Secure Network Computing Services for Lightweight Clients Using Blockchain,” Wireless Communications and Mobile Computing, vol. 2018, pp. 1–12, Nov. 2018, doi: 10.1155/2018/2051693.

[6]. X. Zhou, W. Liang, K. I.-K. Wang, and S. Shimizu, “Multi-Modality Behavioral Influence Analysis for Personalized Recommendations in Health Social Media Environment,” IEEE Transactions on Computational Social Systems, vol. 6, no. 5, pp. 888–897, Oct. 2019, doi: 10.1109/tcss.2019.2918285.

[7]. B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, “Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4118–4149, Jun. 2019, doi: 10.1109/jiot.2018.2875544.

[8]. W. Guo, Y. Zhang, and L. Li, “The integration of CPS, CPSS, and ITS: A focus on data,” Tsinghua Science and Technology, vol. 20, no. 4, pp. 327–335, Aug. 2015, doi: 10.1109/tst.2015.7173449.

[9]. Y. Wang et al., “ContainerGuard: A Real-Time Attack Detection System in Container-Based Big Data Platform,” IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3327–3336, May 2022, doi: 10.1109/tii.2020.3047416.

[10]. Di Wu, Mingsheng Shang, Xin Luo, Yi He, Guoyin Wang and Xindong Wu, "A Data-Characteristic-Aware Latent Factor Model for Web Services QoS Prediction", IEEE Transactions on Knowledge and Data Engineering, DOI 10.1109/TKDE.2020.3014302, 2020.

[11]. W. Xu, W. Fang, Y. Ding, M. Zou, and N. Xiong, "Accelerating Federated Learning for IoT in Big Data Analytics With Pruning, Quantization and Selective Updating," IEEE Access, vol. 9, pp. 38457–38466, 2021, doi: 10.1109/access.2021.3063291.

[12]. L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using an Improved CNN," IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2063–2074, Mar. 2022, doi: 10.1109/tii.2021.3082907.

[13]. B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and Privacy-Preserving Federated Learning With Industrial Big Data," IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6314–6323, Sep. 2021, doi: 10.1109/tii.2021.3052183.

[14]. C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang, and Y. Zhang, "Privacy-Preserving Federated Learning in Fog Computing," IEEE Internet of Things Journal, vol. 7, no. 11, pp. 10782–10793, Nov. 2020, doi: 10.1109/jiot.2020.2987958.

[15]. H. Zhou, G. Sun, S. Fu, L. Wang, J. Hu, and Y. Gao, "Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec," IEEE Access, vol. 9, pp. 43378–43386, 2021, doi: 10.1109/access.2021.3062467.