International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

A Decentralized Security Model for Preventing Data Breaches in Distributed Environments

Rakesh Kumar Mali

Independent Researcher, USA

Email: rakesh.mali80@gmail.com

ABSTRACT: Distributed computing environments became an important component of the contemporary business, cloud computing, Internet of Things and data-centric apps. However, they rest on the huge number of interconnected nodes, which can lead to an increased susceptibility to unauthorized access, insider attacks, poor authentication and huge data breaches. The research study proposes a non-centralized method of security against security breaches in distributed environments due to the reduction in the use of a central authority and increase in trust, transparency and resiliency among the networked systems. The proposed model enhances the security in the various levels through the identity verification, distributed access control, encrypted data sharing, node level authentication and real-time anomaly detection. In the model where security choices are decentralized, then the impact of a compromised node and single points of failures becomes lesser. Cryptographic hashing ensures data integrity and traceability, and access permissions are automated using smart contracts. It is also possible to use this framework of continuously monitoring the activity to forecast the potential suspicious behaviour and also transferring the undesired data prior to the breach happening. The article suggests that decentralization of security architecture can offer superior confidentiality, integrity, availability and accountability of the uncommon distributed infrastructures. Overall, the proposed model offers an extensible and adaptable system of protection of sensitive information on the cloud, edge, and enterprise networks. In its own way, it contributes to the body of knowledge regarding cybersecurity in the sense that it provides a practical security model, which can be compatible with the growing need of trustless, transparent, and breach-resilience distributed systems.

KEYWORDS: Decentralized security, data breach prevention, distributed environments, blockchain security, access control, encryption, anomaly detection.

I. INTRODUCTION

The digital infrastructure that has been adopted in the modern world has been the distributed environment where organizations have shifted to cloud computing, edge computing, Internet of Things (IoT), microservices, blockchain networks, and geographically distributed databases as the location to store, process and transfer information. Various interconnected nodes, applications, users and devices are in charge of the distributed systems compared to the traditional centralized systems where a single, or server is in charge of data and security control [1]. It is more scalable and flexible, it is more challenging to defend sensitive data and performance and availability of its services are greater in this architecture. The risk of unauthorized access, information leakage, insider abuse, identity theft, ransomware and hacking systems are even more critical bearing in mind that the information is being transported to new locations and machines. It is on that ground that the safeguarding against data breaches in distributed environment is an area of contemporary research and practice in cybersecurity [2].

Data breach can be defined as any occurrence where an unauthorised user access, disclosure, modifications, theft or utilisation of confidential, secure or sensitive information took place. Such breaches may be as a result of a weak authentication, weak access control, weak communication media, weak application programming interface, improperly configured cloud services, compromised computers, malware attacks and rogue insiders [3]. These systems are decentralized and it is due to this that it becomes difficult to prevent a breach since there is no information in one location and users are permitted to access sources which are provided by a massive number of different networks, places and machines. Moreover, third-party cloud providers, remote services and foreign APIs are also prevalent in organizations and this contributes to the attack surface. Leveraging this, an attack on one vulnerable point in one node or service will leave the whole system vulnerable to security threat [4].

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

The previous security paradigms tend to be centralized control type in which the policies are executed, authorized and monitored and enforced by a central server or authority. This is effective in small scale or closed setting but highly limited in large scale distributed setting. A single central security system can be an entity of a single point of failure i.e. as soon as the entire command control is weakened, the cybercriminal will find himself/herself in control of the entire network. High performance bottlenecks, low rate of threat detection, poor transparency and fault-tolerance are also high in the centralized models. Moreover, they might be inadequate in terms of trust in the case of different independent parties without the full information of the other party. These restrictions highlight the significance of implementing an enhanced and decentralized security policy [5].

The decentralized security also presents an excellent substitute since it will assist in spreading the security burden among a group of nodes rather than a central node. Some of the actions that can be performed in a network under such a model are the Identity verification, access control as well as data validation and activity monitoring. This will decrease the chances of the system failure as a unit and would render the attackers hard to handle or to destroy the entire infrastructure. Transparency can also be enhanced with decentralized security because all the changes, transactions or access requests can be logged and authenticated by various parties whom can be trusted. It is possible to use technologies that include blockchain, distributed ledger, cryptographic hash, smart contract, the federated identity management and anomaly detection, to build such a model [6].

Decentralized security can, in particular, be applied to the blockchain technology because it offers tamper-resistant logs, distributed consensus and transparent verification. Without authorization, a disseminated configuration can fulfill digital identities, view history, confirmation transactions, and absence of modified data using blockchain. A hacker could hardly modify logs because it is not easy to modify the history of the blockchain unless approved by the network, and it is not easy to hide the evidence about the harmful acts. Smart contracts are also more secure, being able to increase automatic access control and permission enforcements and not requiring a central authority. One of them would be access to data based on certain identity and role requirements, device-based requirements, and time-based requirements via a smart contract.

Another significant aspect of decentralized security model is access control. In most data breach attacks, the attacker relies on the poorly or over-privileged access to sensitive data to gain access. Consequently, the minimum privilege is encouraged where the user together with the devices receive what they can do bare minimum in order to get their work done. Distributed identity verification and policy validation can be employed to support the application of decision-making in the decentralized model to access. This will make sure that all the people will not have everything in terms of permissions of the role of an administrator or server. To achieve a flexible and secure architecture, a context-aware access control, attribute-based access control and context-aware access control can be utilized together with a role-based access control. This would be one of the solutions that would be feasible in cloud and edge computing wherein the user can access the information in more than one machine and location.

The encryption also plays a key role in deterring attacks on data in a distributed system. The data should be locked in transit and rest since the flow of information is usually characterized by nodes and networks. Strong encryption means that intentionally where the attacker taps on data; the attacker cannot decode the data or utilize the data in any possible way unless he/she holds the requisite decryption keys. In distributed environments but a little more difficult to control. It is decentrally secured, and can use distributed key management system to circumvent the issue of cryptographic key being stored in a single location. This minimizes the possibility of exposure to high mass-key and generally improves the privacy of data. Along with it, there is also a cryptographic hash message-digesting algorithm that can be utilized to ensure data integrity and unauthorized alteration.

Real-time tracking and anomalies form another handy need of prevention of breaches. Distributed environments produce amounts of activity log, network traffic or user behaviour information. Under the traditional method of monitoring through manual checks, such complex systems will not be achieved in an appropriate manner to detect more sophisticated threats. Thus there must be decentralized model of security that has built-in threat detection systems and which would detect any suspicious intent of log-in, suspicious data transfer or, privilege escalation, or suspicious node behavior. Potential attacks can also be detected using machine learning and artificial intelligence to determine the patterns. The system can respond to suspicious vicinity by acting automatically on denial, warnings, isolating compromised nodes or further checking.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

The topicality of the given study is in the fact that it is the issue that is obsessed by the growing gap between the developed system and the security preparedness. It has highly centralized and reactive security policies and most organizations are opting to adopt distributed architectures because of their speed, scalability and being cost effective. This inconsistency carries its vices that can be exploited by the attackers. The decentralized security model is more suitable in the context of the distributed environment as it allows spreading trust, enhancing fault resilience, and responsibility. It helps in establishing secure digital environments in the healthcare, banking, education, e-governance, supply chain management, smart cities and industrial internet-of-things, and where sensitive data have to be stored throughout the organization.

The research article title is known as A Decentralized Security Model to Prevent Data Breaches in Distributed Environments and the research objectives will be to develop a security system that will help in minimizing the possibility of occurrence of data breach by decentralizing identity management, access control, encryption, verification by blockchain and anomaly determination, in real time. The paper shall go an extra mile to indicate how security can be designed as part of a distributed system, as opposed to a system being a designated defense mechanism. In this way, the model is going to enhance confidentiality, integrity, availability, trust, and accountability.

To sum it up, a distributed, dynamic and robust security model is necessary in the distributed environment. The current digital systems are not an object of security with the centralized security models to safeguard in response to the contemporary cyber threats. Or even a decentralized security model would be more appropriate since it leaves no failures, it is more open, the rules of access are automatic and the actions of the malevolent can be identified at an early stage. In such a manner, the present study will add to the existing literature on the issue of cybersecurity by serving as a useful and scaled model to avoid data breaches in a complex distributed system.

II. LITERATURE SURVEY

Decentralized security has recently acquired a research point of concern to avoid the IPIP of data breakage in a distributed setting, given that the accessible systems utilize cloud computing, Internet of Things (IoT) and edge networks, a blockchain system and a massive data sharing. The conventional methodology of centralized security design solutions will be susceptible to establishing a single point of failure such that failure of a single server, identity provider or access control database will open the doors of the system. It has been demonstrated in the literature that compliments and leverage can be achieved with blockchain, machine learning, federated learning, smart contracts, attribute-based access control and zero-trust principles, to enhance the confidentiality, integrity, privacy and accountability of distributed systems.

The article by Chen et al. [1] discusses machine learning along with blockchain as a potential remedy to a decentralized and privacy-preservation safe system. Their influence works well since they bridge smart thinking during the analysis of information with the blockchain-coordinated trust. Machine learning can be used as an addition to decision making, and threats are detected and blockchain offers distributed controls and data hardening. This combination can be quite useful, both in decentralized breach prevention since the distributed systems must be automated on what is needed in the secure trust system. The work gives a platform through which machine learning may be applied in identifying suspicious behaviour and blockchain to make security decisions and store transparent and definitive records.

The latter was also complemented by Lu et al. [2] who added blockchain and federated learning to the information exchange in the privacy-sensitive Industrial IoT. This would be opportune since the work of the Industrial IoT environments is to generate delicate data on the various gadgets, factories and the edge nodes in their operation. Federated learning completes the local training rather than transfer of the raw data to the central station and blockchain ensures a secure coordination and integrity of data. This will decrease the dangers of privacy and allow safe communication of disseminated machines. The work might also be used in the existing research, as it demonstrates the mitigation of the data exposure and data flow which is not direct after the given procedures that may be poorly secured.

One of such systems, which uses a blockchain to offer and oversee authorisation of medical data, is MedRec of Azaria et al. [3]. It is a health care based study, which can be applied to the distributed security as the medical records demand high levels of confidentiality, traceability and restricted access. MedRec states that blockchain may be the way to control permission, open history of access and does not require the utilization of centralized databases. The model explains how the patients, providers and institutions can share the records in a safe and responsible manner. This helps

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

to substantiate the idea that the risk of the information leakage in the sensitive setting can be minimized with the help of the inaccessible control.

The article Zyskind et al. [4] is among the initial attempts in privacy decentralizing blockchain to provide the safety of personal information. They were tasked to defeat the old system of centralized data storage where the users are expected to have ownership of their data, with the assistance of the blockchain-based systems. Throughout the paper, it is revealed that the decentralization of the problem of privacy protection, compared to encrimination, should be in terms of control. It is also linked with breach prevention because much of the breaches get realised after the centred depositories of the personal data have been breached. Decentralized privacy will decrease this concentration of risks and more information will be under the control of one of the users.

Kosba et al. [5] suggest Hawk, a smart contract made of a blockchain and privacy-sensitive. Smart contracts could be useful in enhancing security policies in an automated manner, yet a more regular activity of blockchains will offer information as to the character of operations. Hawk can solve this problem by allowing it to have a more privated contract. The other critical part of this contribution is in the form of decentralized security schemes where the task of access control, authentication and permission checks can be automatically fulfilled with the help of smart contracts. These automations should not however give away the sensitive users or transactions data. Smart contracts that are privacy preserving might thus be implemented to guarantee security in policy execution in a distributed setting.

Dorri et al. [6] were also preoccupied with blockchain optimization in the IoT. IoT devices are sometimes resource-constrained devices, but do not necessarily need to be constrained solely by the size of the power, storage, and processing power. Such settings would not be able to back typical blockchain procedures. The lightweight and streamlined blockchain solutions are needed to make sure that the IoT systems are secured: their research has proven that. This can be applied since distributed environments are usually internet-of-things and edge devices that cannot provide sophisticated security operations. A decentralized security model must then possess a trade off between the security of it and efficiency in computer computations.

Among the solutions that Huang et al. [7] came up with was decentralized and data exchange with the IoT, which is trusted by blockchain. They worry about the issue of credibility between distributed devices and companies sharing data without being an organisation: therefore, it is the concern of their masterpiece. These blockchain solutions will offer a solution to authentication of the data transactions and form logs that are difficult to alter. The article helps support the concept that the trust, integrity, and traceability can be enhanced since the information of decentralization is shared. Data transfer of quality will help in circumventing the risk of unauthorized changes, malicious insertion and secrecy modulation of data to avert breaches.

ControlChain is an IoT Authorization Enabler that is an Access Control, which Pinna et al. [8] suggest to use blockchain. The article is of particular interest as the access control is one of the most important components of any data breach prevention. Many devices and services when shared require access permissions. The ControlChain illustrates how blockchain may be used to enact decentralized authorization, as well as keep good access logs. This eliminates the use of centralized access control servers and leads into increased visibility in permissions management.

Di Francesco Maesa et al. [9] also examined the access control using the blockchain and elaborated on the scheme of the management of the access rights keeping the distributed ledger technology in mind. They demonstrate in their work that the access policies, permission, authorization decisions are transparent and free of manipulation and that they are stored in blockchain. The reason is that the hackers will most probably take advantage of least secured or missecured permissions to access sensitive information. Access control is operable on blockchain, by making access control visible, and verifiable to ensure that the access modification is visible and verifiable throughout the system.

The Xiong et al. [10] developed privacy preserving data sharing model of dynamic groups in cloud computing using the attributes. The relevance of the same is that the cloud environments are vulnerable to dynamically changing users, groups and permissions. Attributing based access control allows the opportunity to make decisions based on the user attributes, and the kind of data, condition and context of policy. Not that strict as a role-based access control. In the decentralized security, the attribute based model can be applied in order to enhance the fine grained control of permission and eliminate the unnecessary permission of access which are the greatest contributors of the breach as well.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

The study by Zhang et al. [11] recommended applying an AI-driven data sharing platform of a blockchain in network work. They tie to their solution blockchain-enabled secure sharing to smart network management. The present distributed environment AI tools demand too much of the operating data and the data sharing must be safe. Blockchain has the potential to provide traceability, data integrity and trust in the data sharing process. The above research can be used to realize the safe decentralized information exchange and intelligent tracking, and decision-making.

The Liu et al. [12], suggested blockchain-stop scheme data sharing plan under mobile edge computing, on asynchronous advantage actor-critic learning strategy. The study is relatively up-to-date since the mobile-edge computing demands fast and safe and adaptable decision-making towards sources of information. The reinforcement learning will be implemented to facilitate intelligent control of the resources and blockchain enhances the level of trust and integrity of information. It indicates that adaptive learning could be used in the implementation of decentralized security to enhance performance in dynamically-conditioned environments.

Novo [13] suggested a scaling blockchain of access management of IoT. Scaling is one primary issue of distributed security because an IoT system can consist of thousands or millions of devices. The blockchain can be utilized to enable access control in large IoT networks, such as the one utilized in the Novo case, yet it must be transported in the most preferable way and will not impose a burden on performance. The article can be related to the present research project because it conjectures about the significance of scalable authorization, identity control, and safe communications in the setting of decentralization.

Permission delegation and access control model of IoT imposed by Ali et al. [14] is accomplished through a blockchain, which is referred to as BACI. This is significant as they will be in a position to scan work since delegation of permission is frequently required in a distributed system with users, devices and services having temporary or more generally constrained permissions of access. Weak delegation can turn out to be harmful in the aspect of violations. BACI proves that the blockchain could be utilized to enhance responsible, open and transparent, delegation of permission. This enhances decentralization of access control because the permissions assigned can be viewed and adhere to the policies.

Lastly, Dhar and Bose [15] talked about how the zero trust and blockchain can be applicable to the security of the items of the IoT. In particular, their work is especially applicable in the context of the proposed study because the concept of zero-trust presupposes that no particular user, devices or network components could be trusted per se. Authentication of each access request should be a continuous activity. Integrating blockchain with the zero trust is decentralized and offers benefits of give tampered records and accountability through transparency. This correlates with the main idea of the current paper that the de-centralized security systems are required in the prevention of the data breach in a sophisticated distributed configuration.

On balance, the analyzed articles indicate that blockchain and other decentralized solutions are well-founded, regarding offering secure identity management, data sharing without disrupting the privacy, access, audit, and data breach. But other problems also exist like scalability, cost of calculation, loss of privacy in smart contracts and non-applicability to resource-constrained devices, which are also mentioned in the literature. The problem statement behind the proposed study is based on these studies that incorporated the idea of decentralized identity, access control in smart contracts, encryption, anomaly detection, and the concept of zero-trust that introduced into a single security architecture of distributed environments.

III. FRAMEWORK OF THE PROPOSED DECENTRALIZED SECURITY MODEL

Information security system that will be formulated to counter data breaches in the distributed environment is developed in the form of multi-layered decentralized security model. It is largely aimed at decreasing the reliance of a solitary hub and carries out the security functions in a set of trusted hubs. With a conventional architecture, Authentication, Authorization, monitoring and data checking can be centrally controlled by one central server. This system may be hacked and not configured so and this will bring corruptions in the entire system. The proposed framework will help to cope with this limitation because it is comprised of distributed identity management, distributed access control, encryption, blockchain-based verification, smart contract enforcement, node-level confidence analysis and real-time anomaly detection.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

The architecture is designed such that, it is six-layered, even with six majority-sized layers; user and device layer, decentralized identity layer, access control layer, data protection layer, distributed ledger layer and monitoring and response layer. Verification of the users, devices, transactions and data requests is made possible by the combination of these layers. With an installed zero-trust principle, this model adheres to the principle that every user, device, or node is not trusted, whether they are currently part of the network or not. These access requests will be authenticated to determine, user role, device, location, behavioural policy and security policy.

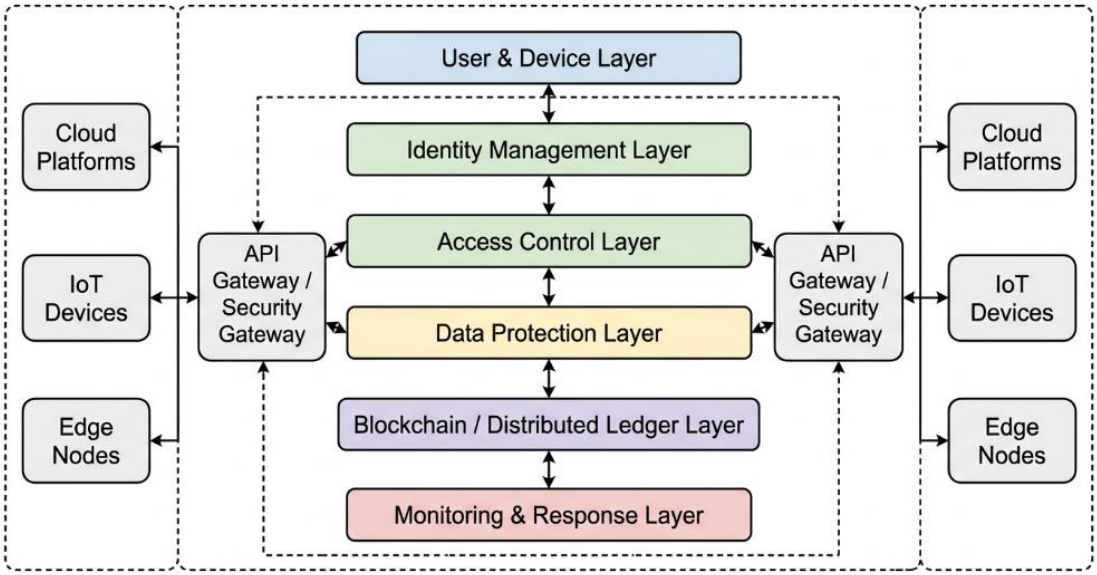

Figure 1: Overall Decentralized Security Architecture

1. User and Device Layer

The first layer of the architecture that interacts in the distributed world is the user, device, application, services and network nodes. They may be in the form of cloud servers, edge devices, IoT sensors, mobile devices, databases, enterprise applications and micro services. Distributed environments may be reached via numerous places and points, so, this layer may be the most susceptible to cyber attacks. If the system is not secured, it can be hacked to have unauthorized entry into the system using weak passwords, insecure devices, outdated software or devices already damaged.

In order to avoid this amount of risk, the architecture required all devices and users to identify themselves prior to gaining access to the network. These receive unique digital IDs and cryptographic authentications are attached to them. To verify the validity of the access attempt, the device fingerprinting, multi factor authentication and the paired key with the public and private keys authenticate the authenticity of the access attempt. This will ensure that the system in use in distribution can only be contacted by the identified and known entities. Such system blocks or isolates an unknown or a suspicious request until it has been verified to be tested to prevent the device making a connection attempt.

2. Decentralized Identity Management Layer

It is a decentralized identity layer, charged with the identity authenticating users, devices, applications and services without necessarily having a single identity provider. Traditional systems will most likely store identity information in central database. Attackers are regarded as a particularly appealing target by attackers because in the event that an attacker merely hacks into an identity server, credentials of thousands or millions of users may be stolen. The fact that it is a drawback of the proposed model does not mean that the proposed model involves the decentralization of identifiers and cryptographic authentication.

This layer spreads the identity records throughout the network and authenticates them in blockchain or distributed ledger networks. Every user or device is given a digital identity and can be authenticated without any personal or

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

organization-related data, which does not necessarily have to be shared. This is helpful in preserving privacy in the authentication. The sensitive credentials are not required to be sent several times and cryptographic evidence can be used to confirm identity. The system will be able to check the validity, active and authorized identity without displaying the entire credential information.

Identity revocation and renewal is also supported by this layer. The distributed network can lose the identity, when the device was lost, a key compromise has been made or when an employee has exited the organization. This revocation property is associated with the ledger, meaning that the entire nodes will instantly be notified that the entity will never be trusted ever again. This minimizes the use of an expired or lost credential.

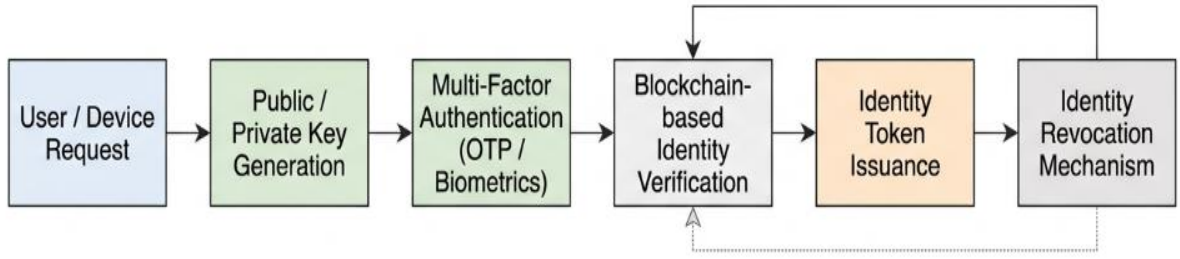

Figure 2: Decentralized Identity and Authentication Flow

3. Distributed Access Control Layer

Access control layer defines access control to a particular resource, which may be either granted to an authenticated user or device. The suggested layout does not have an access control central administrator. Rather, the access control is characterized by distributed policies and implemented with automatically executed smart contracts. This will decrease incidences of human error, escalation of privileges and enhance accountability.

It is a blend of role-based access control, attribute-based access control and context-aware access control. Role based access control offers access privileges based on the position of the user within the organization that may be an administrator, researcher, developer, auditor or external partner. Attribute-based access control also takes other factors into consideration like department, project, type of device, sensitivity of data, location and time of access. Context based access control looks at the current status such as the frequency of use that is abnormal, abnormal location of a login, health and risk level of the device and network.

The implication would be that a user would be free to access a database and be on a machine authorized at the office. Nonetheless, in a scenario where the same user tries to access most of the sensitive information at any time of the night, the user can have the system block the request or authenticate the user. This dynamic access decision making is useful in averting data breach before it actually occurs.

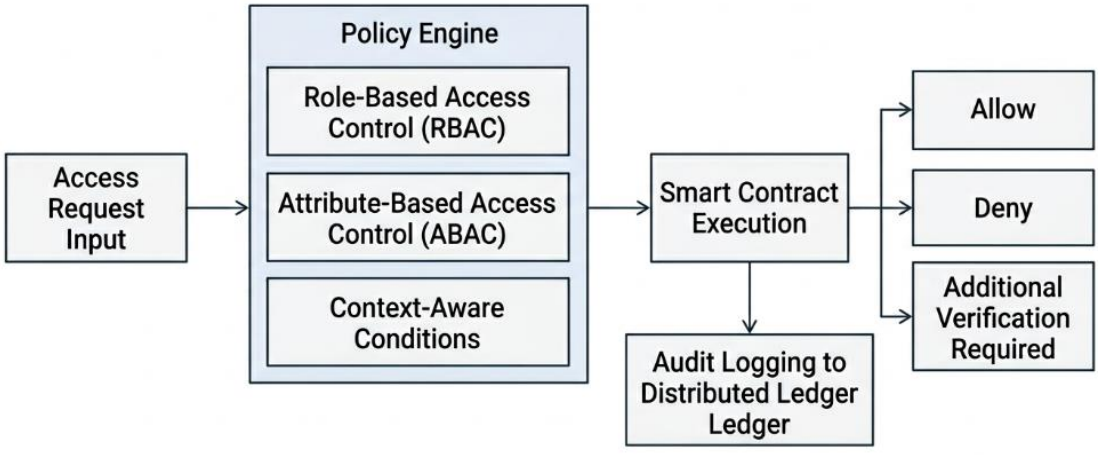

Figure 3: Smart Contract-Based Access Control Mechanism

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

4. Data Protection and Encryption Layer

The data protection layer protects sensitive data in the transmission, processing and storage. Distributed systems flow of information is usually amongst nodes, cloud services, edge system and applications. This motion provides interception, leakage or unauthorized change opportunities. In this way, encryption will be incorporated in the suggested structure.

The data on transit and storage is encrypted with sensitive data. Rest data are data that are stored in data bases, cloud storage or distributed file system. Data in transit refers to the information that is in transit between users, services and nodes among networks. Using strong encryption, no one can intercept and use the data even when intercepted. Cryptographic hashing is also used to ensure integrity of data in the framework. Each data block or transaction is assigned a hash value. The value of the hash will be different in case of any unauthorized change and, therefore, the system will be capable of tracking the interference in real-time.

It has a decentralized key management, as well. The keys are distributed, via the key sharing technique, rather than being stored in a central server where all keys are stored along with the encryption keys. This dampens the malady of key compromise. Although a single node is under attack, the attacker cannot easily access all the encryption keys or the whole dataset. Expiry and key rotation and revocation policies have also been put in place to reduce the long term exposure.

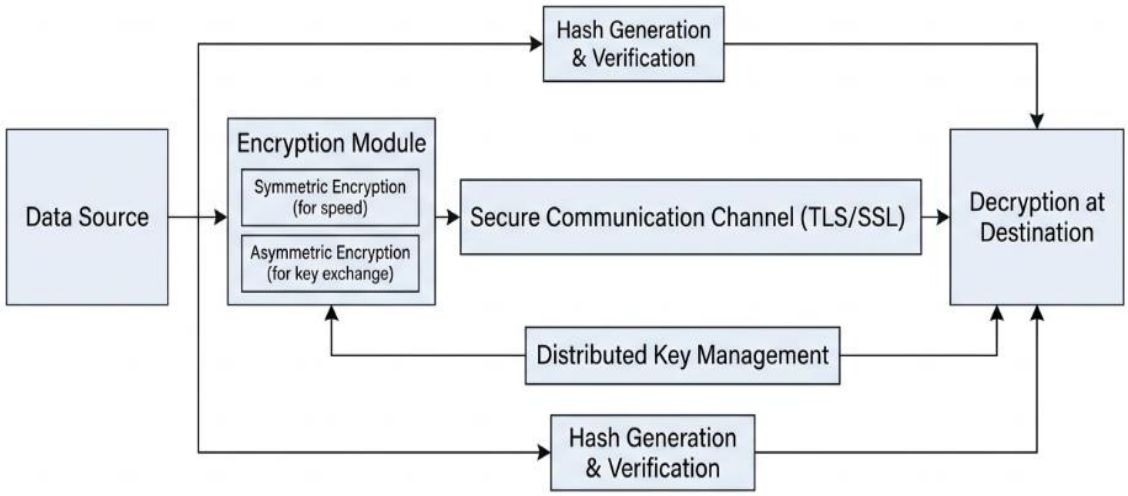

Figure 4: Data Encryption and Secure Transmission Model

5. Distributed Ledger and Blockchain Verification Layer

The distributed ledger layer is not confidential, and can be traced and immutable. Any security operations that need to be stored are kept in a blockchain or distributed registry. These functions might include user registration, authentication, access approval, data transfer, permission changes, node checking and anomalies detected. The ledger books are also copied to several nodes and thus, the attackers cannot easily destroy or alter logs without being detected with ease.

This tier is very important in prevention and detection of data breaches. Most centralized systems also allow attackers to attempt to destroy logs once they have unauthorized access to a system. The proposed system logs are communal and are not editable and malicious activities are difficult to cover. The ledger offers a safe audit history that enables the administrator, and the investigators to know who had viewed what data and when and which device and under what circumstances.

The validation of the transactions is via the consensus mechanism before they are placed in the ledger. It is possible to ensure that little computation is done based on the requirements of the system by lightweight consensus techniques. In the enterprise scenario, permissioned blockchain would be more suitable as only the authenticated user will be in a position to verify their transactions. It makes it more efficient without a lack of trust and safety.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

6. Smart Contract Enforcement Layer
Smart contracts are a computer software that is composed of a sequence of security rules. The proposed model collaborates by using smart contracts to perform access control, identity checks, data-sharing contract, and breach-response. These are automatically deployed/managed contracts that are implemented identically using the distributed environment.

An example is that a smart contract can provide the following statement: only authorized users whose roles are verified, active credentials and safe devices can view confidential files. Granting is subject to fulfilling the requirements. Not fulfilling one of the conditions leads to denial or a more complicated level to explore. Smart contracts can also regulate the number of data downloads, sensitive records being monitored, automatic withdrawal of access to suspicious activity, etc.

Smart contracts will assist in reducing time wastage in the administrative process, and manual decision-making will be eliminated. It also ensures uniformity in implementation of security policies in all the nodes. This is especially essential in those distributed environments where other systems and users may be found in other administrative domains.

7. Real-Time Monitoring and Anomaly Detection Layer
Smart contract is a computer-based code that promotes a set of security regulations. The specified model offers the smart contracts to implement the access control, identity checks, data-sharing contracts, and breach-response. They are automatically deployed/managed contracts which are implemented in the same manner in the distributed environment.

Applying to the case of a smart contract, it will be able to offer the following stateContinuous monitoring and anomaly detection layer: The layer will constantly scan the user behaviour, network traffic, system logs and data access patterns. It aims at identifying the suspicious behaviour before it escalates to a problem of serious data breach. Distributed systems generate high volumes of activity data, which cannot be monitored manually. In this way, the framework implements machine learning-based and automated analytics detection methods.

These normal behavioural patterns are compared with the current behaviour to detect the anomaly by the anomaly detection system. It can identify suspect behaviors such as failed logins, access to non-recognized destinations, the abnormal downloading of data, abnormal change of privileges, abnormal file transfers or communications with suspect nodes. The framework would provide a risk score in cases where there are such activities.

Based on the risk score that the system is capable of assuming, other measures can be taken. The low risk events may be noted down to be referred to. The events of medium-dangerous type could also be verified. High risk may occur and may result in automatic account suspension, isolation of a node, data transfer or notification blockage or notification of an administrator. Such a multi-tiered response can contribute to preventing the threats within a short duration of time and eliminate the threat of huge data leakage.

Admission is granted under the conditions. In case any of the conditions is not met, access is denied or verified. The quantity of data downloads, records being written and automatic right of access to suspicious activity can also be managed with the assistance of smart contracts.

The smart contracts will save time wastage in the administrative process, and reduce use of manual decision making. It also ensures that there is uniformity in implementation of security policy across all the nodes. This is more urgent especially in a distributed system that might contain other systems and users in different administrative areas.

8. Incident Response and Recovery Mechanism
Even when there are successful preventive measures, the distributed systems should be ready to deal with potential security attacks. The proposed model will also have an incident response and recovery mechanism that will be triggered with an attack of breach or a detected breach. Response Process: This includes detection, containment, investigation and recovery and policy improvement.

The infected nodes are removed out of the network so as to avoid further spread in the containment. Revocation of access tokens and cryptographic keys of suspicious accounts. An investigation of the origin and extent of the incident is then carried out with the help of the ledger-based audit trail. Once the threat has been eliminated, the affected systems are recovered using the safe backups and new security policies are implemented to help prevent other attacks.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

IV. PERFORMANCE EVALUATION

Even when there are successful preventive measures, the distributed systems should be ready to deal with potential security attacks. The proposed model will also have an incident response and recovery mechanism that will be triggered with an attack of breach or a detected breach. Response Process: This includes detection, containment, investigation and recovery and policy improvement.

The infected nodes are removed out of the network so as to avoid further spread in the containment. Revocation of access tokens and cryptographic keys of suspicious accounts. An investigation of the origin and extent of the incident is then carried out with the help of the ledger-based audit trail. Once the threat has been eliminated, the affected systems are recovered using the safe backups and new security policies are implemented to help prevent other attacks.

V. FUTURE OPPORTUNITIES

They should also be prepared to handle any security attack even in the presence of successful preventive measures which are in place. An incident response and recovery mechanism will also be a part of the proposed model and it will be activated with an attack of breach or a detected breach. Response Process: This consists of detection, containment, investigation and recovery and policy improvement.

The infected nodes are ejected out of the network or in order to prevent further transmission in the containment. Cancellation of access tokens and cryptographic keys of suspicious accounts. The ledger-based audit trail is then used to conduct an investigation of the origin and extent of the incident. After the threat has been removed, the affected systems are restored using the safe backups and new security policies are enacted to aid in preventing other attacks.

VI. CONCLUSION AND FUTURE WORK

This study paper proposed a decentralized security model and in curbing the data breach in the distributed environment. This paper has determined that security threats that the modern distributed systems like cloud, edge, IoT and enterprise networks are prone to are increasing because of the availability of various access points, interconnectivity of nodes, third parties providing services and volumes of data traffic. The classical centralized security models can no longer be entirely satisfactory as they introduce the concept of the single point of failure, performance and low level transparency bottlenecks. Therefore, the idea of resilience, trust and accountability must be augmented with decentralization.

The proposed model will consist of decentralized identity management, distributed access control, encryption, blockchain-based verification, smart contracts and live anomaly detector. This is a set of components that are brought together to come up with the identification of users and devices, safeguard of confidential data, uncovering of suspicious behavior and the production of audit audit records that cannot be changed. The framework increases the confidentiality, integrity, availability and accountability by ensuring that security decisions are not confined in a specific, individual, dependent node that can be compromised over but are shared among trusted nodes. It can also assist continuous validation, which is a crucial aspect of insider threats, devices of compromised and abnormal access behaviour identification.

As far as the analysis of the activity carried out by the model is concerned, it can be promoted breach avertance, accuracy of authenticity, efficiency of the access control, and data integrity, resilience of the systems, and scaling. Unlike in decentralized security where additional computing power and appropriate settings are required, the returns in this scenario are enormous, and the safety of data, availability of services, and trust are the most important. This model would be of great assistance to any business such as healthcare, banking, education, e-governance, smart cities and supply chains systems.

The second work step could be focused on the implementation and testing of the suggested paradigm to actual distributed environment. The prototype can be tested to determine the actual performance under various sizes of the network, attack conditions and volume of transactions. It could be also incorporated to the future research to use the artificial intelligence and machine learning to reach greater heights of detecting anomalies and preventing the predictive threats. Moreover, the possibility of lightweight blockchain consensus mechanisms to reduce the latency and computing overhead must be taken into account. Zero-knowledge proofs, homomorphic encryption and secure multi-party computation are the privacy saving technologies that can be adopted to improve the model. Overall, the research

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

|| Volume 7, Issue 1, January-February 2024||

DOI:10.15662/IJRPETM.2024.0701011

to be carried out in the future should streamline the setup and transform it into practical and scalable and industry-ready solution to ensure distributed computing.

REFERENCES

[1] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Seattle, WA, USA, Dec. 2018.
[2] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.
[3] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. Int. Conf. Open Big Data*, Vienna, Austria, Aug. 2016.
[4] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.
[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Security and Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.
[6] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-of-Things Design and Implementation (IoTDI)*, Pittsburgh, PA, USA, Apr. 2017, pp. 173–178.
[7] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based on blockchain," in *Proc. 3rd IEEE Int. Conf. Computer and Communications (ICCC)*, Chengdu, China, Dec. 2017, pp. 1180–1184.
[8] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in *Proc. IEEE Global Communications Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–6.
[9] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Proc. IFIP Int. Conf. Distributed Applications and Interoperable Systems*, Berlin, Germany: Springer, 2017, pp. 206–220.
[10] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2739–2750, 2019.
[11] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for AI-powered network operations," *Journal of Communications and Information Networks*, vol. 3, no. 3, pp. 1–8, 2018.
[12] L. Liu, J. Feng, Q. Pei, C. Chen, Y. Ming, B. Shang, and M. Dong, "Blockchain-enabled secure data sharing scheme in mobile-edge computing: An asynchronous advantage actor–critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.
[13] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
[14] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in Internet of Things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, 2019.
[15] S. Dhar and I. Bose, "Securing IoT devices using zero trust and blockchain," *Journal of Organizational Computing and Electronic Commerce*, vol. 31, no. 1, pp. 18–34, 2020