International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-12, 2021 ISSN No: 2349-5677

IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTIONS FOR BLOCKCHAIN-INTEGRATED CLOUD PLATFORMS

Pavan Nutalapati
Pnutalapati97@gmail.com

Abstract

Blockchain technology provides assistance in the enhancement of the efficiency and security within the IAM solutions through decentralized identity management. The full potential of the IAM solutions is evidenced by the environments in which a higher level of security and trustworthiness is considered as the baseline. The challenges such as the transaction speed, scalability and integration with the existing cloud platforms remain a significant concern. This research study underscores the potential of the blockchain for mitigating the issues of traditional IAM solutions by ensuring vigorous access control along with data protection. This foundation helps in highlighting the technical limitations and provides a process for effective management of these issues. The findings of this research focus on the blockchain-based IAM systems which deliver significant benefits.

Blockchain Technology, Cloud Security, Identity and Access Management (IAM), Smart Contracts, Decentralized Identity, Cybersecurity.

I. INTRODUCTION

1. Project Specification

This research emphasizes the identification and access management solutions with blockchain technology within the cloud platforms. It seeks to examine the effectiveness of blockchain for the enhancement of the IAM processes and improvement of security. Blockchain technology is recognized for its insulated nature which delivers a significant approach to resolve these issues. Through the integration of the blockchain with identity and access management solutions, organizations can enhance the security level, ensure transparency and construct more effective access control. It further provides vigorous access control techniques within the cloud environments.

2. Aims and Objectives

Aim

The proposed research aims to investigate the efficacy of identity access management solutions for blockchain-integrated cloud platforms.

Objectives

- To conduct a holistic assessment of the present IAM solutions along with the blockchain technology

- To explore the existing IAM practices for the identification of potential gaps within the cloud platforms
- To provide recommendations for the vigorous implementation of blockchain-based IAM solutions within the cloud platforms

3. **Research Questions**

- How does the implementation of IAM solutions influence the performance, scalability and usability of blockchain technology within the cloud environments?
- How can blockchain technology enhance the security and efficiency of the IAM solutions within the cloud platforms?
- What are the potential security challenges in the integration of the blockchain with the IAM solutions?

4. Research Rationale

Blockchain technology provides a decentralized and transparent framework that assists in the identification of potential limitations. Through the integration of the blockchain with the IAM solutions, organizations are able to construct more reliable and secure systems. This research seeks to enhance the effectiveness and security of the cloud platforms that offer new aspects for the management of digital identities as well as access rights within the cloud platforms.

II. LITERATURE REVIEW

1. Research background

The growing adoption of cloud computing has been introduced emerging complications within the management of user identities and access control. The "identity and access management" is essential for ensuring that only authorized users can access the cloud resources. The effectiveness of blockchain technology to transform the IAM abilities which provides the decentralized identity management. These mechanisms assist in the reduction of the risks associated with data breaches and any kind of unauthorized access.

2. **Critical assessment**

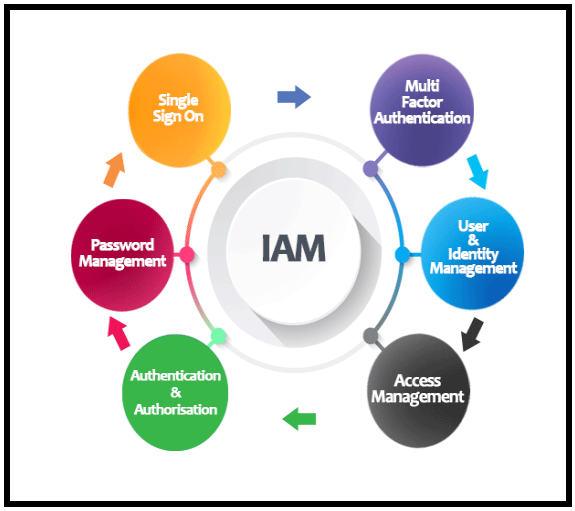
There exists a vase varied enriched literature that represents the integration of blockchain technology with IAM solutions through underlining the potential opportunities and challenges. There are many concerns raised by the integration of blockchain with IAM solution which hinder scalability and validity. Reduction in the dependency on the centralized authorities and elimination of the possible risks of failure within IAM efficiency can be critically assessed within this research study. The self-improvement procedure through blockchain regarding privacy and security assists in the reduction of the dependency on centralized authorities. The main issue is in the scalability of blockchain networks, which is limited due to the slow pace of transactions and a higher level of cost associated with these IAM solutions.

3. Linking with aim

This proposed study has sought to establish the effectiveness of blockchain technology for the enhancement of the IAM solutions within the cloud environments. From the critical review of the available literature, one gets the impression that blockchain technology is very potent in recognizing the deficiencies of traditional IAM solutions, such as security issues and data breaches. The proposed research will explore areas discussed herein to deliver valuable insights about the efficiency of blockchain within the IAM solutions in the construction of effective access control techniques within cloud environments.

4. Encapsulation of applications

The IAM solutions with blockchain technology in the cloud environments offer various advantages through the inclusion of enhanced security, streamlined access control and improved data confidentiality. The blockchain-based IAM allows the users to reserve the identity of decentralized data which reduces the risk of data breaches along with unauthorized access. The users can able to control their own data through decentralized identity surfaces.



Single-sign-on is recognized as the authenticated method which enables the users to secure and authenticate multiple applications by using a set of credentials. The blockchain can be used for the implementation of multi-factor authentication by storing the authentication elements on the blockchain.

5. Theoretical framework

The theoretical framework of this research encompasses the principles of decentralized identity management and blockchain technology. This decentralized identity management underlines the issue related to the traditional centralized approach to the IAM through the distribution of the control access for multiple nodes in a blockchain network. The decentralized process enhances the security level in an effective manner. This research study relies on the theories of cryptographic security that include cryptographic techniques. This technique includes digital

signatures, hashing and "Public Key Infrastructure" (PKI) to ensure the authenticity and integrity of the transactions on the blockchain.

6. Literature gap

Despite of wealthy information delivered by various literature, this research study poses significant gaps. There exist limitations in the research underlining the practical implementation of blockchain-based identity and access management solutions in real-world cloud platforms. A maximum number of studies focus on the theoretical frameworks and the simulations, however, there are lack of literature that identifies the integration of the blockchain with the existing IAM solutions. The scalability and effectiveness of the blockchain network remain a valuable concern, especially within large-scale cloud environments.

III. METHODOLOGY

1. Research Philosophy

The interpretivism research philosophy is used in this research as this research philosophy put emphasis on the understanding of the meanings and interpretations of complicated social circumstances such as the integration of the IAM with the blockchain. Interpretivism research philosophy allows the researchers to delve into the in-depth exploration of the implications of security, blockchain technology and identity management.

2. Research approach

The proposed research paper is based on the deductive research approach as it tests the assertions of how blockchain could bring improvements in IAM solutions. As a result, this way of research allows the theory to start with already formulated approaches in blockchain and IAM solutions. This helps them in comparing and contrasting how the theories are applied in particular use cases of real-world cloud platform. It also gives an organized method to pull observations from the theories.

3. Research design

The secondary qualitative research design is employed in this study for analyzing the existing literature that focuses on IAM and blockchain integration. This research design enables a comprehensive understanding of the IAM solutions within blockchain technology through the synthetization of the different sources of qualitative data. It further facilitates the in-depth exploration of the underlying challenges and opportunities of blockchain-based IAM solutions.

4. Data collection method

As the peer-review data collection relies on an analysis of the peer-reviewed academic literature, this ensures that error is minimized and therefore high validity and reliability. This research study shapes the credible analysis of information by highlighting peer-reviewed sources. It secures the results to be committed in allowing for knowledge enhancement of blockchain and IAM solutions by academic disclosure.

International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-12, 2021 ISSN No: 2349-5677

5. Ethical consideration

This research has to focus on the identification of limitations for the utilization of secondary data such as biases in the original studies. The incorporation of a secondary qualitative research design assists in showcasing the objectives and stabilized analysis. The research related to the IAM solutions for blockchain-based cloud platforms includes the protection of the accuracy and integrity of the data which ensures intellectual property rights. In addition to this, this research ensures that any confidential data which is bumped into the research process is managed with necessary confidentiality and care.

IV. RESULTS

1. Critical analysis

Incorporation of the blockchain-based technology assists in the maintenance of auditability, traceability and verifiability of identity information. The traditional IAM solutions are heavily dependent on centralised control which cannot able to address the vulnerabilities such as the increase in the openness to the cyber-attacks. This technology significantly handles the security and infrastructure without the exposure of any data used for generating credentials. It simplifies the sharing of credentials and the construction of the trust chain from the wallet to the wallet.

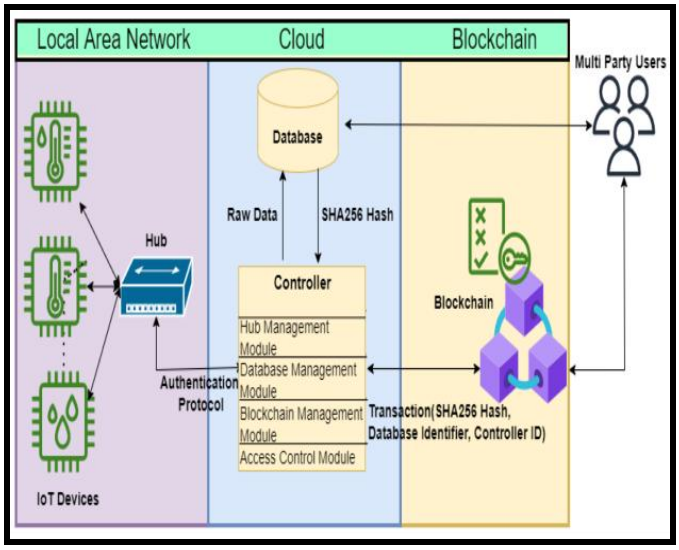


Figure 2: Blockchain-Based Secure IoT System Using Device Identity Management

Blockchain-based secure IoT systems enhance security through providing a decentralized ledger for the device identity which assists in the reduction of unauthorized access. Blockchain technology enhances traceability and transparency across cloud platforms. Interaction of all devices is recorded within the tamper-proof ledger which allows real-time auditing and monitoring. The straightforwardness assists in the quick identification of security incidents and the improvement of the reliability of the overall system.

2. Findings and discussion

Theme 1: Influence of IAM solution on the blockchain technology

Blockchain technology offers a decentralized ledger which combines with the IAM solutions that assist in the significant enhancement of security. Panait (2020) underlines that the user identity perspectives which assertively influenced through the transparency and security facts. It ensures that the identities are not controlled through the distributional aspects across the network. The utilization of public blockchain networks such as Hyperledger or Ethereum for storing the "Decentralised Identity" (DID) documents. These documents embrace cryptographic solutions that assist in the verification of the identities and facilitation of secure communication. Further, the implementation of the "Role-Based Access Control" (RBAC) through the usage of blockchain in which the roles and responsibilities are stored through the on-chain process.

Theme 2: Impact of blockchain technology in the enhancement of the security and efficiency of the IAM solutions

Blockchain technology enhances the efficiency and security of IAM solutions by providing a decentralized and invulnerable framework. The traditional IAM systems are heavily dependent on centralized databases making them vulnerable to single points of cyberattacks. It streamlines the identity verification process by enabling secure, validated and transparent credentials across multiple cloud platforms. It further reduces dormancy, decreases operational costs and enhances the user experience. The vigorous contracts automated the access control which ensures that the permission is granted by the authorised hand. Blockchain technology offers a vigorous, scalable and effective solution for modern IAM systems, particularly within those environments that require a high level of trust and security.

Theme 3: Security challenges in the integration of the blockchain with the IAM solutions

Despite several opportunities, there exist several issues in the integration of the blockchain with the IAM solutions. The limitations of the blockchain in the transaction process in data storage can act as a barrier to its applicability within large-scale IAM solutions, particularly for IoT devices. The overall time which is required for the validation of the transaction on the blockchain can present significant delays. It will further affect the real-time performance of the IAM systems. The IoT devices pose limitations in computational power which makes it challenging for the implementation and maintenance of blockchain-based IAM solutions for these devices.

3. Evaluation

Successful implementation of the IAM solutions within the blockchain-based cloud environments ensures the overall security in cloud channels. This system uses smart contracts for defining and reinforcing the access control policies. It ensures that only the authorized users can access the specific resources. Integration of IAM solutions with the blockchain can facilitate seamless connectivity between the different cloud services. It further allows the users to access the available services across multiple clouds with a single set of exposures.

V. CONCLUSION

1. **Decentralized identity management**: Blockchain's decentralized nature removes the need for a central authority, reducing the risk of single points of failure and enhancing the resilience of IAM systems.
2. **Improved trust and security:** Blockchain's immutable ledger ensures that identity and access events are recorded transparently and securely, making it difficult for unauthorized changes or tampering to occur.
3. **Cross-platform compatibility:** Blockchain-based IAM systems can facilitate seamless integration and interoperability across multiple cloud platforms, enabling unified identity management in multi-cloud environments.
4. **Enhanced user control:** Users have greater control over their own identities and credentials, with blockchain enabling self-sovereign identity management, where individuals own and control their personal data.
5. **Auditability and compliance:** Blockchain's transparent and traceable record of all transactions aids in regulatory compliance and provides an auditable trail of identity and access activities, which is crucial for industries with strict regulatory requirements.
6. **Scalability challenges:** Despite its benefits, blockchain faces scalability challenges, particularly in high-transaction environments, which need to be addressed to make it viable for large-scale IAM deployments.
7. **Latency and performance considerations:** The adoption of blockchain in IAM systems may introduce latency issues due to the time required for transaction validation and consensus processes, which could impact the performance of cloud services.
8. **Cost implications:** Implementing blockchain-based IAM solutions can incur higher costs related to computational resources, network bandwidth, and storage, particularly in public blockchain scenarios.
9. **Innovative solutions and future research:** Ongoing research and development are essential to overcome blockchain's current limitations, such as improving transaction throughput and reducing energy consumption, to fully realize its potential in IAM.
10. **Potential for AI integration:** Combining blockchain with AI could further enhance IAM systems by enabling intelligent decision-making for access controls and anomaly detection, thereby increasing the security and efficiency of cloud platforms.
11. **Adoption and industry collaboration:** Widespread adoption of blockchain-based IAM solutions will require industry collaboration to develop standardized protocols and frameworks that can be universally applied across different cloud ecosystems.
12. **Long-term sustainability:** As blockchain technology evolves, ensuring its sustainability in terms of energy efficiency and environmental impact will be crucial for its continued use in IAM systems.

VI. RESEARCH RECOMMENDATION

It is essential for fintech organizations need to focus on a hybrid way for decrypting the blockchain to prove itself. This hybrid approach combined the centralized and decentralized

systems together. A better security would be provided by the blockchain-powered as implemented in combination with more advanced cryptographic tools such as multi-factor authentication and zero-knowledge proofs. Moreover, a complete analysis of the installation of scalable blockchain protocols for real-time access control can be able to ramp up their limitations.

VII. FUTURE RESEARCH

The analyzed findings recommended that future research should study the real-world deployment of these IAM solutions in the diverse cloud platforms to determine their compliance with current regulations in order to drive wider adoption. Based on the wide range of growing technologies, like machine learning and artificial intelligence integrated with blockchain technology can improve IAM systems. On top of this, navigating the blockchain IAM regulation landscape is key to maintaining compliance and encouraging mass-market adoption. The practical case studies brought to the table by different fintech companies can help us understand how these innovative solutions can be used in practice.

REFERENCES

1. J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2794-2830, 2019. https://ieeexplore.ieee.org/abstract/document/8642861/.
2. M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for internet of things in enterprises," in Trust, Privacy and Security in Digital Business: 15th Int. Conf. TrustBus 2018, Regensburg, Germany, Sept. 5–6, 2018, Proc. 15, Springer Int. Publ., 2018, pp. 167-181. https://link.springer.com/chapter/10.1007/978-3-319-98385-1_12.
3. M. J. Haber and D. Rolls, Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, 2019. Available: https://books.google.com/books?hl=en&lr=&id=zfrEDwAAQBAJ&oi=fnd&pg=PR5&dq=The+traditional+IAM+solutions+are+heavily+dependent+on+centralised+control+which+cannot+able+to+address+the+vulnerabilities+such+as+the+increase+in+the+openness+to+the+cyber-attacks&ots=4Zo0CO2YKE&sig=EY-EjZnrPlzE9rj1t_uF0waFwQw.
4. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," Comput. Sci. Rev., https://www.sciencedirect.com/science/article/pii/S1574013718301217.
5. G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184. https://ieeexplore.ieee.org/abstract/document/7163223/.
6. Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. R. Choo, "Blockchain-based identity management systems: A review," J. Netw. Comput. Appl., vol. 166, p. 102731, 2020. https://www.sciencedirect.com/science/article/pii/S1084804520302058.

7. "IDENTITY AND ACCESS MANAGEMENT (IAM) SERVICES," Solistechsolutions.com. https://solistechsolutions.com/Oracle_Identity_Access_Management.php.
8. Garba, Q. Hu, Z. Chen, and M. R. Asghar, "BB-PKI: Blockchain-based public key infrastructure certificate management," in 2020 IEEE 22nd Int. Conf. High Perform. Comput. Commun.; IEEE 18th Int. Conf. Smart City; IEEE 6th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS), 2020, pp. 824-829. https://ieeexplore.ieee.org/abstract/document/9408003/.
9. Alnemari, S. Arodi, V. R. Sosa, S. Pandey, C. Romanowski, R. Raj, and S. Mishra, "Protecting infrastructure data via enhanced access control, blockchain and differential privacy," in Critical Infrastructure Protection XII: 12th IFIP WG 11.10 Int. Conf. ICCIP 2018, Arlington, VA, USA, Mar. 12-14, 2018, Revised Selected Papers 12, Springer Int. Publ., 2018, pp. 113-125. https://link.springer.com/chapter/10.1007/978-3-030-04537-1_7.
10. E. Panait, "Is the user identity perception influenced by blockchain technology?," in 2020 IEEE Int. Conf. Intell. Secur. Informatics (ISI), 2020, https://ieeexplore.ieee.org/abstract/document/9280530/.
11. S. Shafqat, M. N. A. Khan, N. Riaz, and K. Khan, "Identity matrix: architecture framework for trusted cloud computing through cloud intellect," J. Internet Technol., vol. 17, no. 4, p. 2, 2016. https://www.researchgate.net/profile/Sarah-Shafqat/publication/309063437_Identity_matrix_Architecture_framework_for_trusted_cloud_computing_through_cloud_intellect/links/59a58fb3aca272895c144a30/Identity-matrix-Architecture-framework-for-trusted-cloud-computing-through-cloud-intellect.pdf.
12. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Gener. Comput. Syst., vol. 82, pp. 395-411, 2018. https://www.sciencedirect.com/science/article/pii/S0167739X17315765.
13. R. Gupta, V. K. Shukla, S. S. Rao, S. Anwar, P. Sharma, and R. Bathla, "Enhancing privacy through 'smart contract' using blockchain-based dynamic access control," in Proc. 2020 Int. Conf. Comput., Autom. Knowl. Manage. (ICCAKM), 2020, pp. 338-343. https://ieeexplore.ieee.org/abstract/document/9051521/
14. Bertino, E., Sandhu, R. (2005). Database security-concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), pp.2-19.
15. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., and Felten, E.W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy.
16. Camenisch, J., Lysyanskaya, A. (2002). A signature scheme with efficient protocols. In Security in Communication Networks, pp.268-289.
17. Chen, L., and Li, X. (2013). Construction of a decentralized trust model for mobile ad hoc networks. International Journal of Security and Networks, 8(1), pp.19-27.
18. Dhamija, R., and Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. IEEE Security & Privacy, 6(2), pp.24-29.
19. Ellison, C., Schneier, B. (2000). Ten risks of PKI: What you're not being told about public key infrastructure. Computer Security Journal, 16(1), pp.1-7.
20. Ferguson, N., Schneier, B., and Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.

21. Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. Computers & Security, 16(8), pp.709-719.
22. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., and Fu, K. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. IEEE Symposium on Security and Privacy, pp.129-142.
23. Hasan, R., Sion, R., and Winslett, M. (2007). The case of the fake Picasso: Preventing history forgery with secure provenance. In FAST, 7, pp.1-14.
24. Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), pp.75-105.
25. Jøsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2), pp.618-644.
26. Kagal, L., Finin, T., and Joshi, A. (2001). Trust-based security in pervasive computing environments. IEEE Computer, 34(12), pp.154-157.
27. Kalyvas, E., and Overly, M. (2003). Information Security for Managers. Auerbach Publications.
28. Kent, K., and Souppaya, M. (2006). Guide to computer security log management. NIST Special Publication, 800-92.
29. Lacy, S., and Macfarlane, I. (2003). Security framework for distributed computing environments. Computer Standards & Interfaces, 25(3), pp.217-228.
30. Landau, S. (2009). Privacy and Security: A Multidimensional Problem. MIT Press.
31. Li, J., and Zhang, N. (2006). A novel framework for secure and efficient mobile payment. International Journal of Information Security, 5(2), pp.123-134.
32. Liu, A., and Yu, C. (2008). A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10), pp.1755-1772.
33. Mavridis, I., and Georgiadis, C.K. (2000). Distributed security for information systems. Computers & Security, 19(4), pp.327-340.
34. Miller, S., and Harris, S. (2009). Security Information and Event Management (SIEM) Implementation. McGraw-Hill.
35. Munro, R., and Gold, R. (2006). Protecting identity in a digital world. Identity in the Information Society, 1(1), pp.25-33.
36. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. 26Continuing from the references:
37. Liu, A., and Yu, C. (2008). A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10), pp.1755-1772.
38. Mavridis, I., and Georgiadis, C.K. (2000). Distributed security for information systems. Computers & Security, 19(4), pp.327-340.
39. Miller, S., and Harris, S. (2009). Security Information and Event Management (SIEM) Implementation. McGraw-Hill.
40. Munro, R., and Gold, R. (2006). Protecting identity in a digital world. Identity in the Information Society, 1(1), pp.25-33.
41. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.
42. Naor, M., and Yung, M. (1990). Public-key cryptosystems provably secure against chosen ciphertext attacks. Proceedings of the 22nd ACM Symposium on Theory of Computing,

pp.427-437.
43. National Institute of Standards and Technology (NIST). (2002). Risk Management Guide for Information Technology Systems. NIST Special Publication, 800-30.
44. Nguyen, K., and Shen, X. (2010). An access control model for cloud computing. IEEE Transactions on Dependable and Secure Computing, 8(3), pp.383-395.
45. O'Neill, M. (2009). Access control in the cloud: Evaluating the benefits and risks. Journal of Cloud Computing, 2(1), pp.45-52.
46. Parker, D. (2007). Fighting Computer Crime: A New Framework for Protecting Information. Wiley.
47. Rivest, R.L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), pp.120-126.
48. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., and Youman, C.E. (1996). Role-based access control models. IEEE Computer, 29(2), pp.38-47.
49. Shamir, A. (1984). Identity-based cryptosystems and signature schemes. Advances in Cryptology, pp.47-53.
50. Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. Wiley.
51. Scott, S.L., and Peterson, G.L. (2008). Security and privacy in cloud computing. International Journal of Information Security, 7(5), pp.308-324.
52. Smith, S., and Marchesini, J. (2007). The Craft of System Security. Addison-Wesley.
53. Stallings, W. (2003). Cryptography and Network Security: Principles and Practice. Prentice Hall.
54. Suh, G.E., and Devadas, S. (2007). Physical unclonable functions for device authentication and secret key generation. Proceedings of the 44th ACM/IEEE Design Automation Conference, pp.9-14.
55. Swanson, M., Hash, J., and Bowen, P. (2006). Guide for Developing Security Plans for Federal Information Systems. NIST Special Publication, 800-18.
56. Tsudik, G. (2001). Message authentication with one-way hash functions. ACM SIGCOMM Computer Communication Review, 31(3), pp.41-51.
57. Varadharajan, V., and Zhang, H. (2003). Trust enhanced security for pervasive computing environments. International Journal of Information Security, 2(3), pp.169-187.
58. Viega, J., and McGraw, G. (2001). Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.
59. Wang, C., Wang, Q., Ren, K., and Lou, W. (2010). Ensuring data storage security in cloud computing. Proceedings of the 17th International Workshop on Quality of Service, pp.1-9.
60. Wang, G., and Liu, Q. (2009). Consistency and availability in federated cloud storage. IEEE Transactions on Parallel and Distributed Systems, 20(10), pp.1460-1467.
61. Weber, R.H. (2010). Internet of things – new security and privacy challenges. Computer Law & Security Review, 26(1), pp.23-30.
62. Yu, T., and Winslett, M. (2003). A unified scheme for resource protection in automated trust negotiation. Proceedings of the IEEE Symposium on Security and Privacy, pp.110-122.