Section A-Research paper
ISSN 2063-5346

Social Media Security Techniques uisng Blockchain over cloud computing

Dr. Nilesh Uke
Professor, Trinity Academy of Engineering, Pune, India
nilesh.uke@gmail.com
Dr. Priya Pise
Associate Professor,
Indira College of Engineering and Management, Pune, India
priya.pise@gmail.com
Mr. Ashish Dudhale
Department of Electronics and Telecommunication Engineering, Research scholar, JJT University, Rajasthan, India and Assistant Professor, AIT, Dighi, Pune, India
ashish.dudhale@gmail.com
Dr Akhilesh Kumar Mishra,
Research Guide, JJT University, Rajasthan, India
agars2012@yahoo.in

Abstract
Blockchain has developed into an unstoppable disruptive technology that has the ability to revolutionize industries. Ignoring it might put enterprises at a competitive disadvantage. The most popular uses of Bitcoin, apart from its initial use in finance, are supply chain management and electronic voting systems. Less attention is paid to blockchain applications related to information and cybersecurity, particularly from a corporate standpoint. This knowledge vacuum is filled in this article by investigating blockchain as a use case for identity management within an enterprise. The article provides a thorough background to help readers comprehend the subject, including how true the statements are. Centre on it, particularly the promise of blockchain to address issues with identity management, are supported by facts or are merely the product of hype. The 69 publications that were qualitatively chosen from reputable academic sources were summarized using the research process known as meta-synthesis. Theoretical basis for some of the statements presented is generally apparent, although it is not always favourable to the corporate setting. The study shows that blockchain technology is at an early stage of development, which raises the question of whether it is truly practicable for enterprises to implement distributed identity management based on blockchain technology. Toe-BDIDM is a research model that is suggested to direct more study.

Introduction

The importance of data integrity issues is highlighted by the fact that they can have a significant negative impact on mission-critical systems that rely on accurate data [1]. Protecting the digital system (such as a network, website, database, and application) utilising the data by applying efficient identity and authentication management is one of the key elements in maintaining data integrity.

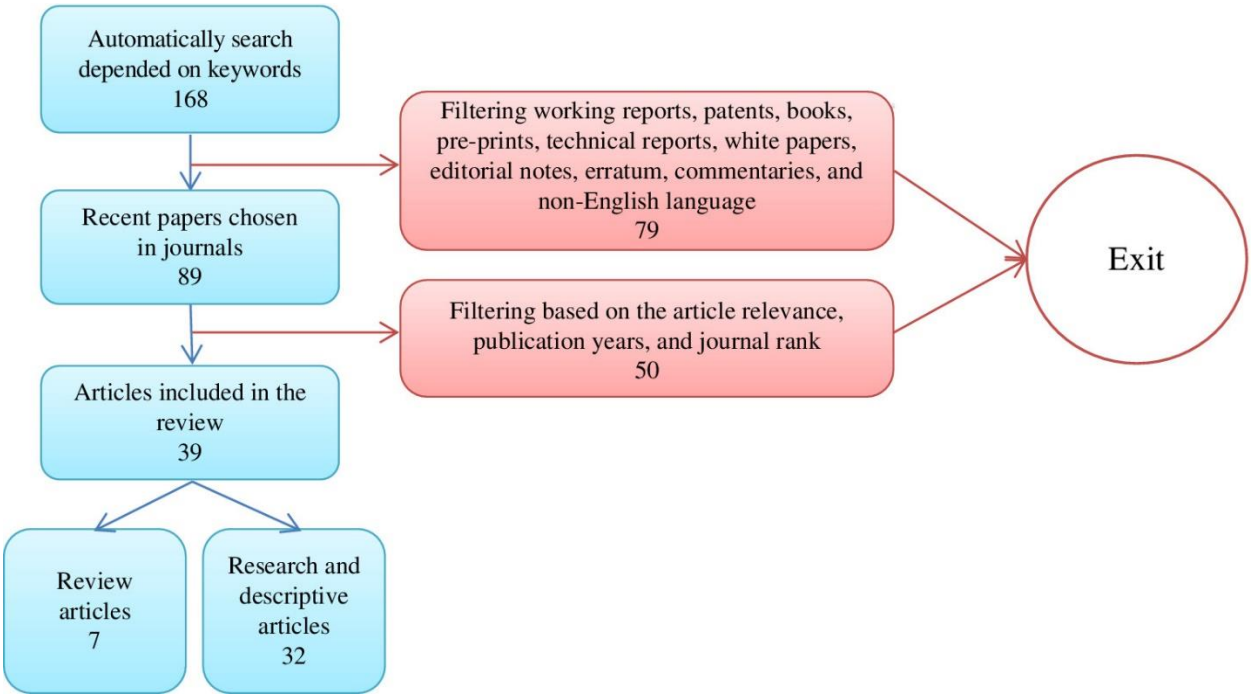

Fig.1: Social Media Security Techniques uisng Blockchain over cloud computing flow.
Only those with permission can use the system and potentially access the data in this way. However, data breaches and the repercussions they cause continue to happen, casting considerable doubt on contemporary IDM systems [2]. For instance, a Serianu analysis found that cybercrimes and financial losses are more prevalent in Africa [3]. According to the IBM 2019 Cost of a Data Breach Study, the average.

Methodology

This explorative study employed the meta-synthesis approach of "qualitative meta-aggregation and meta-summary" research. The latter aims to condense knowledge and "distil information to draw conclusions" [9] while developing "refined meanings, exploratory theories, and new concepts." It is founded on an interpretative methodology and seeks to "rigorously synthesize qualitative research findings" in order to create information that may be applied generally [10]. All research types—quantitative, qualitative, empirical, conceptual, and review—opted for a realist meta-synthesis by integrating constructive and interpretative methodologies to get beyond their particular limits. Both meta-synthesis and systematic reviews have some commonalities.

Majority of the guidelines used throughout the evaluation process are predefined [11]. The major distinction between a systematic review and a review procedure that was performed several times to fulfil the richness criterion of a qualitative research and develop the review scope. Meta-analysis was not appropriate because it tends to emphasise objectivity above richness [10], is linear, and often evaluates data across quantitative research "to identify statistically significant results" [9]. The review scope, data location (databases), search keywords, selection criteria, exclusion criteria, and methodologies and processes of analysis and synthesis were all set guidelines in this study. +e initial phase consisted of framing the review exercise, determining the scope of the review.

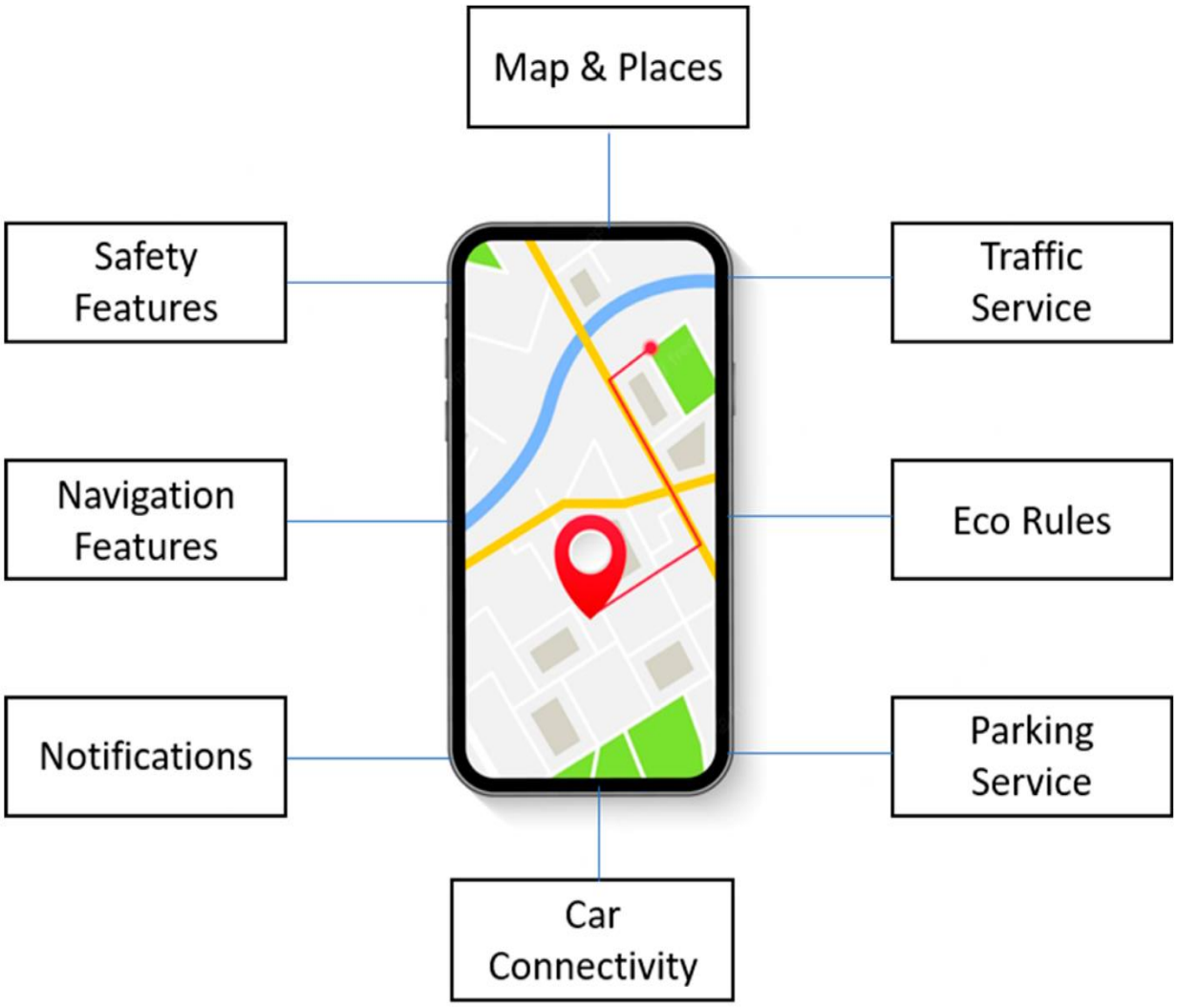

Fig.2: Social Media Security Techniques uisng Blockchain over cloud computing Process.

Results and Discussion

This section provides a narrative report of the review results. Figure 3 illustrates how the study is organized to address the key subjects that fall under its purview. IDM basics, issues that must be resolved, and the development of IDM models to resolve IDM challenges are all covered in MT1. Blockchain principles, such as promoting and restricting factors, are covered in MT2. The idea, IDM model, blockchain implementation, and capacity to manage IDM difficulties are some of the topics covered by MT3 in their discussion of the viability of BDIDM in companies. MT4 evaluates the veracity of the BDIDM statements stated during the review and explains factors that impact BDIDM adoption in organisations based on the technologyorganisation-environment theory. +e following sections of the review gives the fundamentals of IDM and highlights some critical IDM challenges needing to be addressed.

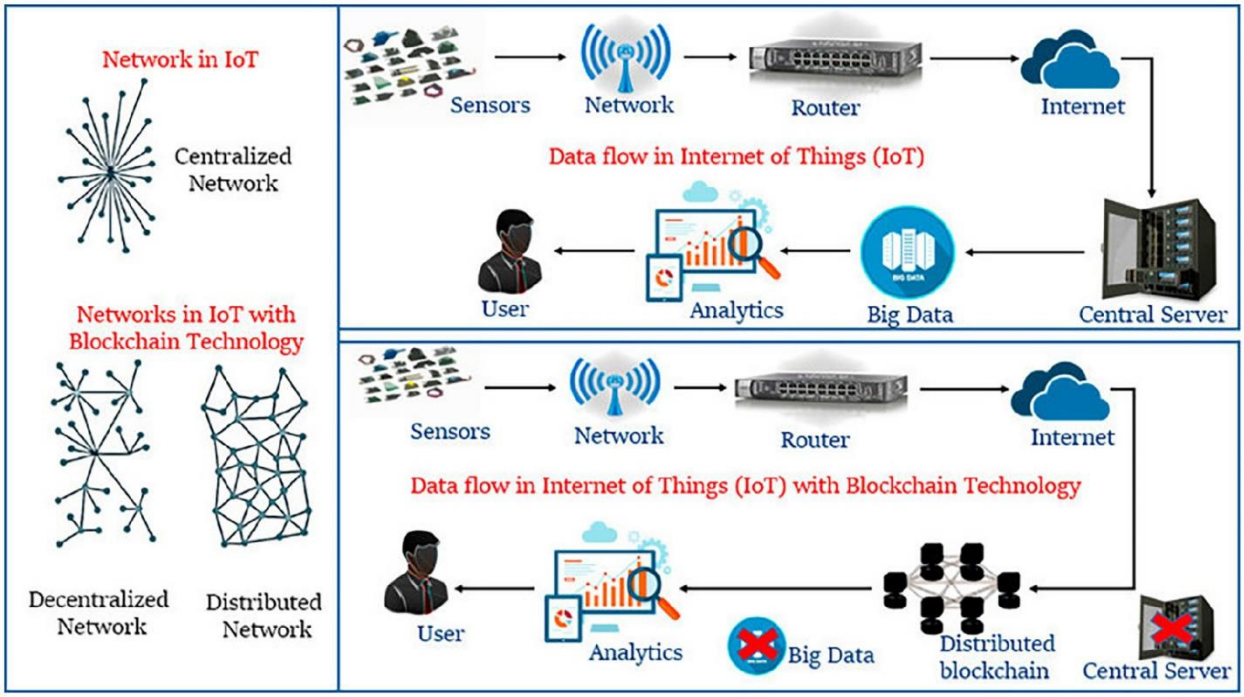

Fig.3: Social Media Security Techniques uisng Blockchain over cloud computing Method.

The IDM System Architecture has flaws. Due to the fact that centralized IDM uses a single server to hold identification information, it introduces a serious single point of failure (SPOF) vulnerability. Identity information is disclosed and the server could no longer be accessible after it is hacked [2-2]. A well-known security risk management theory is SPOF. It implies that when a system's total operation depends on a single node, there is a significant chance that the entire system will fail if that node goes down. According to a few research, "multicity redundancy technology" [2-3] would mitigate the SPOF vulnerability and achieve reliability and resilience in digital systems [2-4]. Redundancy involves having a duplicate copy of the database on every node, generally known as distribution [2-5]. +at is why distributed systems, such as Blockchains, have “arguably no single point of failure vulnerability”

Centralized IDM.

Users "cannot sign on across different domains" because traditional IDM systems are "based on central authorities" that are typically separated from one another and create trust silos [7]. Because of this, "users are forced to rely on a different central service to manage their identity data in each different domain" [2]. For each separate service, a user has an account (a username, password, or biometric). It is "inefficient and onerous for users (forcing them to remember numerous different private information) even while this is practically perfect from the company perspective (because it offers an organisation total control over the usage of "its" digital assets), authentication information)” [2]. Centralized IDM systems use protocols such as RADIUS and Kerberos, providing authentication of both individuals and applications on a dedicated server.

Self-Sovereign Identity (SSI).

Blockchain is used by a typical user-centric IDM to acquire SSI systems [4-1]. In this architecture, there is no one owner of the decentralized identity provider system. It "does not

represent a trusted third party and allows digital identities that are under the full control of the associated subject" [4-2]. This is the reason why SSI is increasingly being portrayed as the IDM systems' "privacy-respectful solution" [7]. Using a software wallet that is loaded on their device (such a smartphone), identity data is saved on the user side, technically on their particular block [4-3]. Users have the option to register, recover, and even delete their data if they decide not to use it any more.

Enterprise Blockchain (EB).

A "permissioned blockchain used by any organisation" is what the EB idea refers to [48]. However, one of the causes for EB's acceptance delays may be the lack of clarity on its applicability in the actual world. Blockchains haven't been used to solve sufficiently significant business challenges, despite the expertise of technology experts [4-9]. The Blockchain Technology Transformation Framework (BTTF), developed by Demir et al., was designed to assist executives and managers in assessing blockchain-based solutions for industrial innovation. Likewise, Labazova [4-7] proposed the framework for assessing blockchain implementations in organisations, regardless of its use case. However, despite its potential impact on business that could promote its adoption, EB is still subject to various constraints.

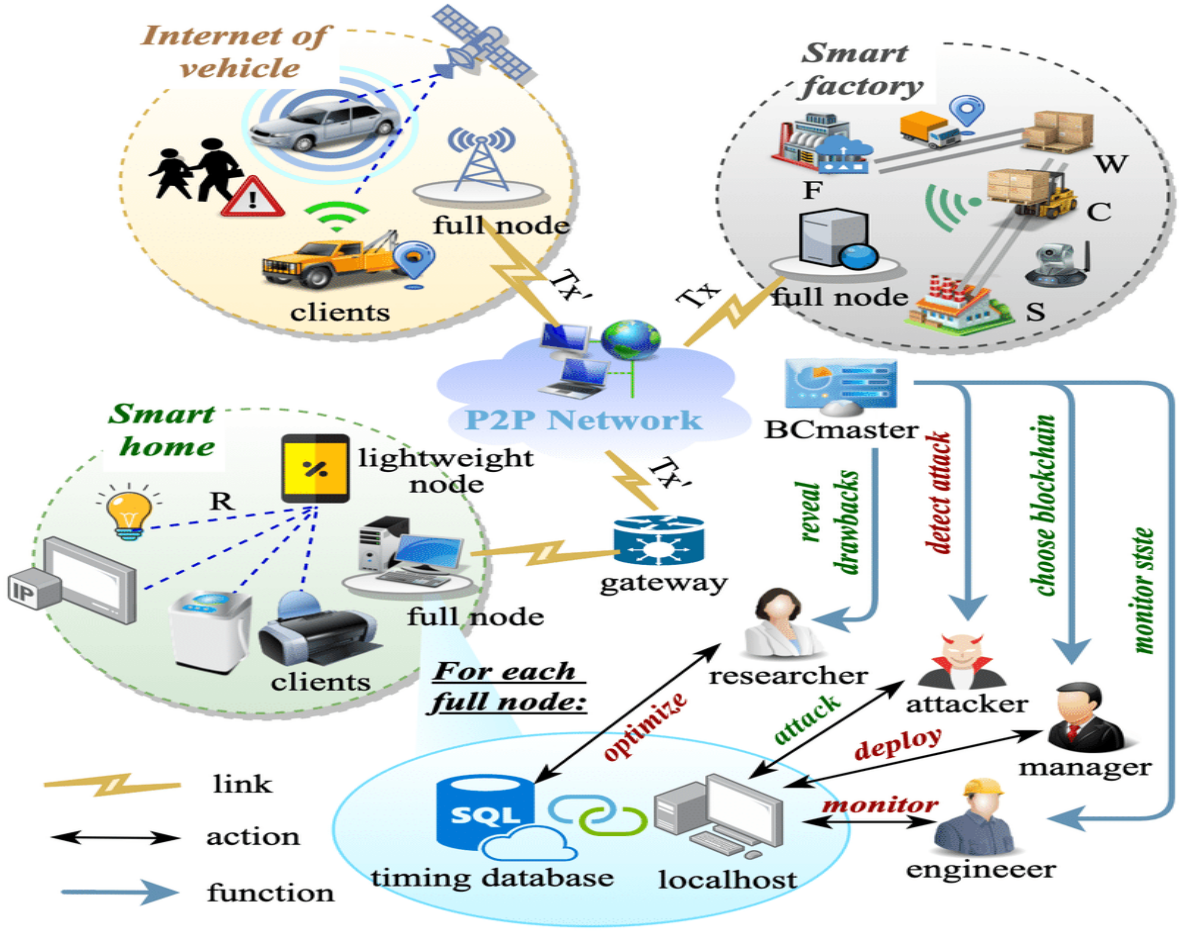

Fig.4: Social Media Security Techniques uisng Blockchain over cloud computing Process.

According to further studies, "blockchain-based identity and access management systems can address some of the key challenges" related to the secure cloud [5]. IoT devices are recognised,

authorised, and linked through cloud servers, which frequently conduct processing and storage over the Internet, making the "current centralized cloud model of IoT security" problematic since the IoT is reliant on the cloud. Operations moving via the Internet can be manipulated. The phrase "Blockchain sovereign identity solutions" can help solve these issues, and some projects and experiments that focus on IoT identity problems are undergoing [3-1]. A pragmatic point of view would argue that the disruptive capabilities of BDIDM may be beneficial “only in those scenarios where the advantages outweigh the drawbacks” [2]. In other words, when considering a benefit of BDIDM, such as privacy-preserving, one “should question whether it would add value, eliminate a weakness, provide an advantage, or preclude a threat from competitors”.

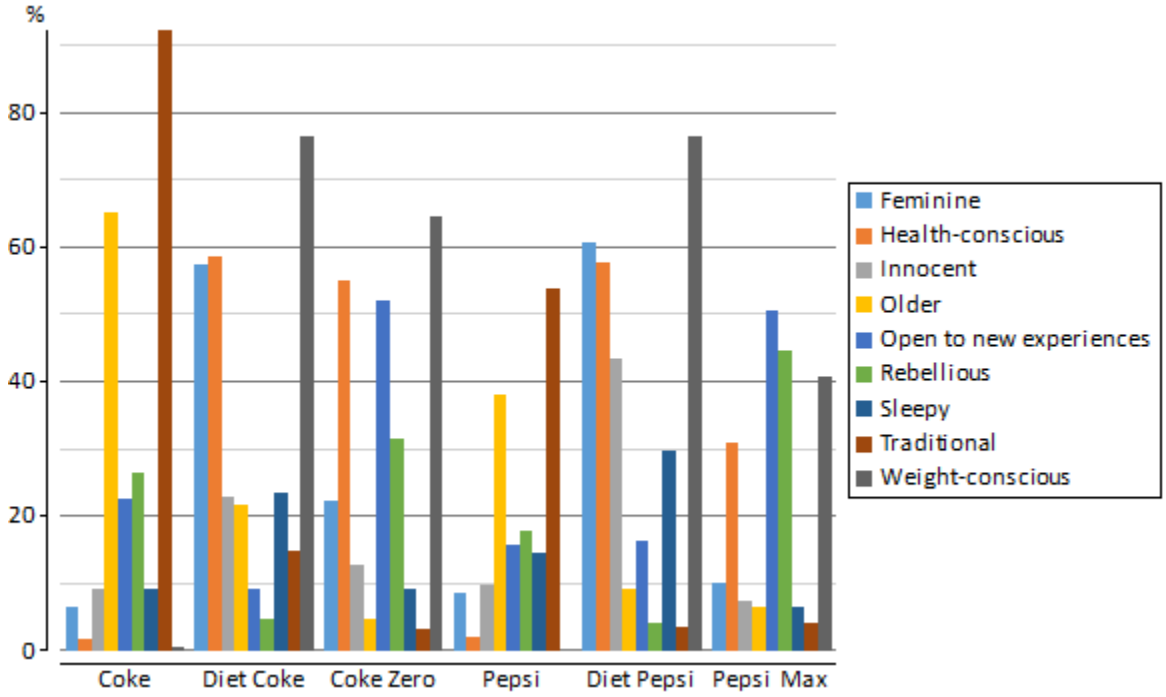

Fig.5: Social Media Security Techniques uisng Blockchain over cloud computing Graph

Conclusions

This section summarises the results while taking into account the already mentioned study's aims and scope. Additionally, see the section on BDIDM characteristics. Security, privacy, trial ability, and Observability are requirements for a blockchain. - Consistency BDIDM preparedness, integration, complexity, governance, and standardization Infrastructure and capabilities - IT capabilities - BDIDM capabilities Organisational traits Organisation - Linkage with employees - The existence of product evangelists Organisational structure, support from top management, and leadership and communication Organisational preparedness Financial resources - Awareness Organisation size External environment Industry and market environment - Industry pressure - Competition intensity Support environment - Vendors support - Skill labour – Consultants.

Regulatory environment - Government regulation - Compliance with standards BDIDM adoption TOE-BDIDM. As suggestions for further research, 14 Security and Communication Networks outlines numerous knowledge gaps found in the literature before outlining the main

limitations of the study. This study looked at the literature to find out more about the history of the BDIDM as a blockchain use case. The goal was to comprehend the subject, particularly how useful the adoption of BDIDM was from an organisational standpoint. The investigation implied whether or not the assertions made about blockchain technology, particularly its ability to help firms with IDM difficulties, were true. Additionally, the study hinted at whether BDIDM was as disruptive to companies as believed (in comparison to conventional IDM systems).

References

1. S. Shetty, C. A. Kamhoua, and L. L. Njilla, Blockchain for Distributed Systems Security, John Wiley & Sons, Hoboken, New Jersey, United States, 2019.
2. D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," Journal of Parallel and Distributed Computing, vol. 138, pp. 99–114, 2020.
3. P. Musuva-Kigen, F. Mueni, and D. Ndegwa, Africa Cyber Security Report 2016, Serianu Cyber +reat Intelligence Team, Nairobi, Kenya, 2016.
4. IBM-Security, "IBM: cost of a data breach report," Computer Fraud & Security, vol. 2019, no. 8, p. 4, 2019.
5. N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017.
6. M. Kopparberg, "Blockchain-based identity management: a survey from the enterprise and ecosystem perspective," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1008–1027, 2019.
7. J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Sarmatia, "Privacy-preserving solutions for blockchain: review and challenges," IEEE Access, vol. 7, pp. 164908–164940, 2019. [8] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain," ACM Computing Surveys, vol. 53, no. 1, pp. 1–39, 2020.
8. D. Finfgeld-Connett, A Guide to Qualitative Meta-Synthesis, Routledge, New York, NY, 2018.
9. C. Romero, S. Ventura, M. Pechenizkiy, and R. Baker, *Handbook of educational data mining*, CRC Press, 20122
10. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, Cambridge, Mass, USA, 2016.
11. C. Romero and S. Ventura, "Educational data mining: a survey from 1995 to 2005," *Expert Systems with Applications*, vol. 33, no. 1, pp. 135–146, 2007.
12. C. Romero and S. Ventura, "Educational data mining: A review of the state of the art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 40, no. 6, pp. 601–618, 2010.
13. Shweta Pal, Kiran More, Priya Pise, "Content-Based Deduplication of Data Using Erasure Technique for RTO Cloud", 2018 International Conference on Advances in Communication and Computing Technology (ICACCT) Pages- 109-113
14. Aaqib Ahmad, Nikita Khandelwal, Akshay Konapure, Priya Pise, "Detection of Wildlife Using Thermal Camera and Passive Infrared Sensor by Smart Hybrid Robot", International Journal of Research in Engineering, Science and Management Volume-2, Issue-1, January-2019
15. Priya Dudhale Pise, Nilesh J. Uke "Efficient Security Framework for Sensitive Data Sharing and Privacy Preserving on Big-Data and Cloud Platforms", International

Conference on Internet of things and Cloud Computing March 2016Article No.: 38Pages 1–5https://doi.org/10.1145/2896387.2896423

16. C. Romero and S. Ventura, "Data mining in education," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 3, no. 1, pp. 12–27, 2013.
17. R. S. Baker and Y. Yacef, "The state of educational data mining in 2009: A review and future visions," *JEDM-Journal of Educational Data Mining*, vol. 1, no. 1, pp. 3–17, 2009.
18. A. Peña-Ayala, "Educational data mining: A survey and a data mining-based analysis of recent works," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1432–1462, 2014.
19. B. Bakhshinategh, O. R. Zaiane, S. ElAtia, and D. Ipperciel, "Educational data mining applications and tasks: A survey of the last 10 years," *Education and Information Technologies*, vol. 23, no. 1, pp. 537–553, 2018.
20. H. Aldowah, H. Al-Samarraie, and W. M. Fauzy, "Educational data mining and learning analytics for 21st century higher education: A review and synthesis," *Telematics and Informatics*, vol. 37, pp. 13–49, 2019.
21. Parikshit Narendra Mahalle, Gitanjali Rahul Shinde, Priya Dudhale Pise, Jyoti Yogesh Deshmukh ,"Foundations of data science for engineering problem solving", Publication date 2022 Publisher Springer
22. C. Piech, J. Bassen, J. Huang et al., "Deep knowledge tracing," in *Annual Conference on Neural Information Processing Systems (NIPS)*, C. Cortes, N. D. Lawrence, D. D. Lee, M. Sugiyama, and R. Garnett, Eds., pp. 505–513, Curran Associates, Inc., 2015.