2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT) | 979-8-3315-1857-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/CE2CT64011.2025.10939863

Blockchain for Cybersecurity_ Securing Data Transactions and Enhancing Privacy in Digital Systems

Durgam Rajababu
Department of EEE, School of Engineering
SR University
Warangal, Telangana, India
durgamrajababu@gmail.com

S. Surya
Sri Ramachandra Faculty of Engineering & Technology (SRET)
Sri Ramachandra Institute of Higher Education & Research
Porur, Chennai – 600116, India
surya@sret.edu.in

Mrutyunjay Padhiary
Department of Agricultural Engineering, Triguna Sen School of Technology
Assam University
Silchar, Assam – 788011, India
mrutyu@gmail.com, ORCID ID: 0000-0002-2236-568X

Harshadkumar Modi
Computer Engineering
Government Polytechnic
Gandhinagar, India
harshadsmodi@gmail.com

Abstract— The feasibility of using blockchain technology as a method to improve cybersecurity through data security transactions and users' anonymity is discussed in this paper. It scans network traffic, sings out abnormities, and uses the clustering approach to find cybersecurity risks. The identified evidence points to the prospects of blockchain to disrupt threat management and enhance the resilience of digital landscapes against cyber threats.

Keywords— ***Blockchain Technology, Cybersecurity, Data Privacy, Clustering Techniques, Network Traffic Analysis***

I. Introduction

Blockchain technology has proved to be a reliable solution to cybersecurity threats, especially by providing decentralized, immutable and transparency data transactions. This paper focuses on the use of blockchain in the protection of data transactions and the privacy of such transactions in Computer systems and Networks, and the effectiveness of blockchain in the protection against data breaches, unauthorized accesses and cyber security threats.

The objective of the study is centred on the analysis of blockchain security in maintaining cybersecurity. The framework evaluating the significance of data privacy and security in digitalized environment is developed in regards to blockchain-enabled security. The study is going to contribute in the implications of blockchain security in cybersecurity.

II. Literature Review

Blockchain, initially established for creating cryptocurrencies such as Bitcoin, has expanded its view as a general technology. Blockchain in cybersecurity comes with a decentralized ledger, whereby it is almost impossible to perform alterations on the records since they are recorded as they are recorded on a plain sheet of paper [1]. Scholars are identifying a growing interest in how blockchain can help ward off cyber threats such as DDoS attacks, data leakage, piracy, and identity theft.

Some of the studies discussed incorporate blockchain with digital identity management systems as follows. Decentralized identification by use of Blockchain is made secure contrary to the central authority prone to hacks. The frameworks of self-sovereign identity based on the blockchain allow the user to manage the data but remain private.

In the area of secure data exchange, smart contracts programmable code run on the blockchain that executes transactions without third parties make certain that an exchange of data between different parties is sensitive and cannot be interfered with. Using supply chains or financial operations as an example, it is clear that blockchain adds and improves transparency and reliability.

However, there are drawbacks associated with blockchain technology, among them technological restrictions, such as scalability and high energy utilization. One of the fundamental consensus mechanisms ill-used in many blockchains is the Proof-of-Work (PoW) consensus algorithm, which requires much processing power [2]. To overcome these challenges, researchers are proposing new models such as Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT).

This literature also reviews the literature on the use of blockchain in privacy preservation. Secrecy technologies like zero-knowledge proofs and homomorphic encryption preserve blockchains' decentralization and its properties, the transference of assets without trusting any central authority [3]. Thus, it turns to show how aspiring it is to protect user identity and delicate information in industries such as healthcare and IoT devices through blockchain solutions.

III. Methodology

The method here calls for the examination of the ability of blockchain to protect data transactions and improve privacy drawn from a dataset of cybersecurity threats and blockchain solutions. Sub-processes are initial data pre-processing to determine potentially dangerous cyber threats and further comparison of existing security measures with blockchain ones. Measures like transaction integrity, privacy and attack are summarized [4]. In addition, the apportionment of

analysis on real-life examples of blockchain integration in various industries such as finance, healthcare, and IoT is provided to evaluate the cases in practice. The results inform the application of blockchain in cybersecurity having described its advantages and disadvantageous within this paper.

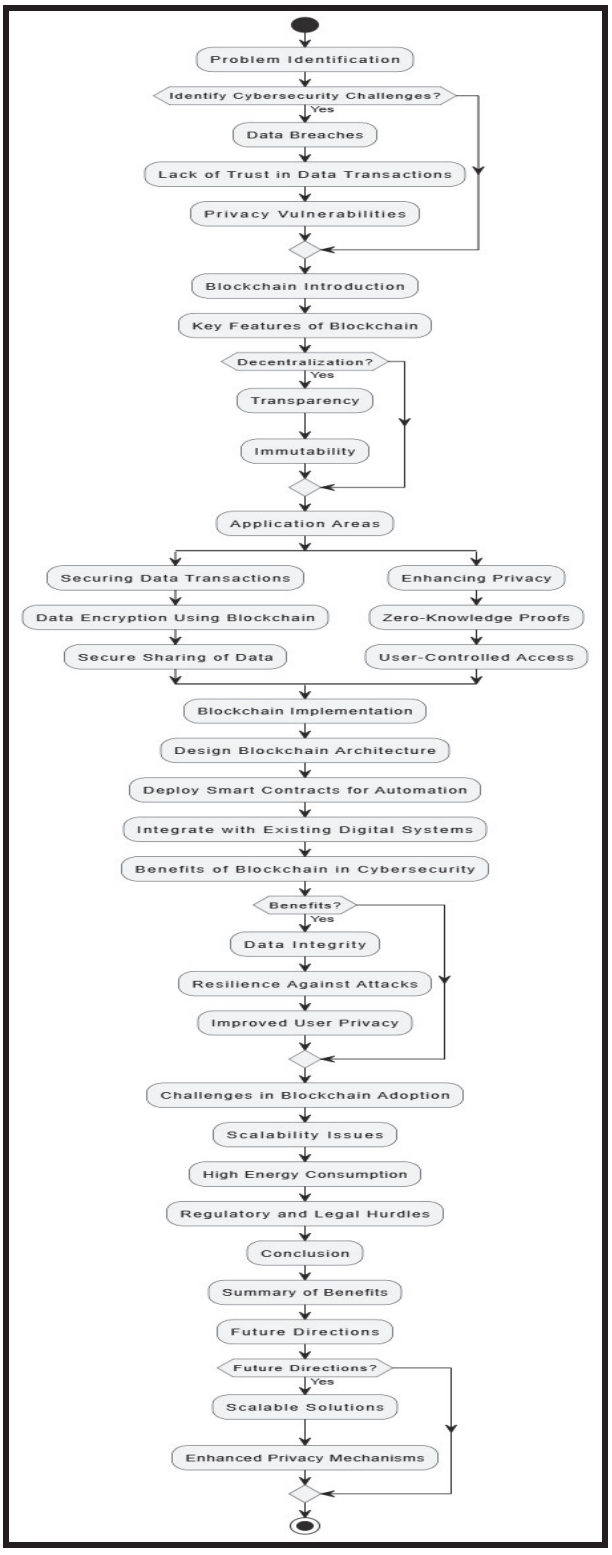
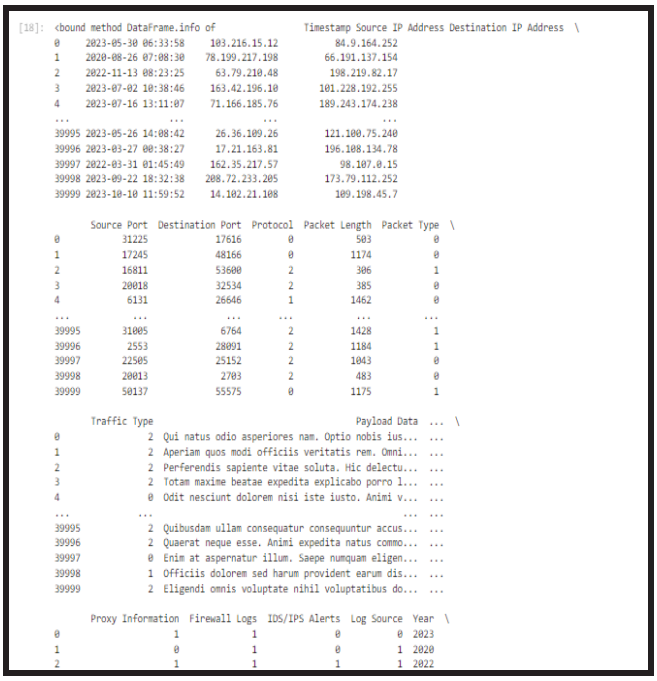


Fig. 1 Methodological Framework of The Blockchain System

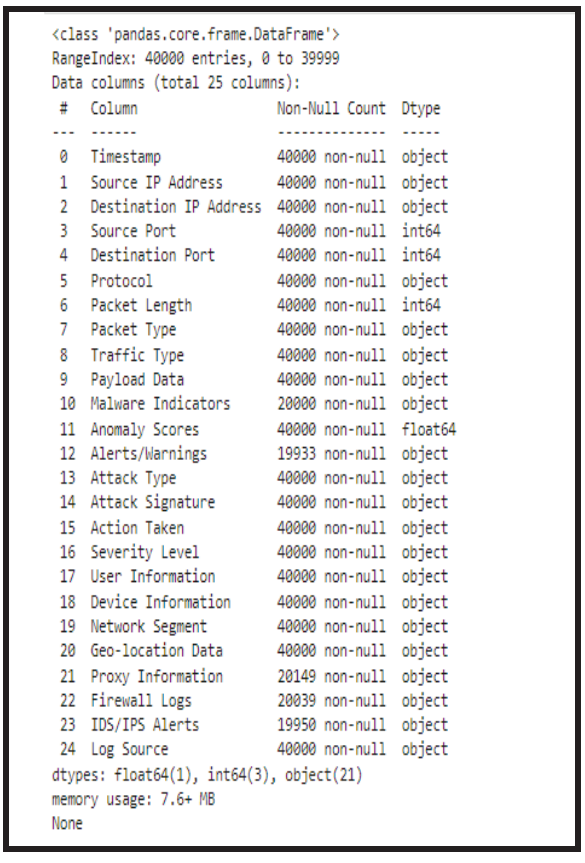
IV. ANALYSIS



```
[18]: <bound method DataFrame.info of                Timestamp Source IP Address Destination IP Address  \
0     2023-05-30 06:33:58     103.216.15.12          84.9.164.252
1     2020-08-26 07:08:30     78.199.217.198         66.191.137.154
2     2022-11-13 08:23:25      63.79.210.48          198.219.82.17
3     2023-07-02 10:38:46     163.42.196.10         101.228.192.255
4     2023-07-16 13:11:07     71.166.185.76         189.243.174.238
...                   ...               ...                     ...
39995 2023-05-26 14:08:42      26.36.109.26         121.100.75.240
39996 2023-03-27 00:38:27     17.21.163.81          196.108.134.78
39997 2022-03-31 01:45:49     162.35.217.57          98.107.0.15
39998 2023-09-22 18:32:38     208.72.233.205        173.79.112.252
39999 2023-10-10 11:59:52     14.102.21.108          109.198.45.7

       Source Port  Destination Port  Protocol  Packet Length  Packet Type  \
0            31225             17616         0            503            0
1            17245             48166         0           1174            0
2            16811             53600         2            306            1
3            20018             32534         2            385            0
4             6131             26646         1           1462            0
...            ...               ...       ...            ...          ...
39995        31005              6764         2           1428            1
39996         2553             28091         2           1184            1
39997        22505             25152         2           1043            0
39998        20013              2703         2            483            0
39999        50137             55575         0           1175            1

       Traffic Type                                       Payload Data  ... \
0                 2  Qui natus odio asperiores nam. Optio nobis ius...  ...
1                 2  Aperiam quos modi officiis veritatis rem. Omni...  ...
2                 2  Perferendis sapiente vitae soluta. Hic delectu...  ...
3                 2  Totam maxime beatae expedita explicabo porro l...  ...
4                 0  Odit nesciunt dolorem nisi iste iusto. Animi v...  ...
...             ...                                                ...  ...
39995             2  Quibusdam ullam consequatur consequuntur accus...  ...
39996             2  Quaerat neque esse. Animi expedita natus commo...  ...
39997             0  Enim at aspernatur illum. Saepe numquam eligen...  ...
39998             1  Officiis dolorem sed harum provident earum dis...  ...
39999             2  Eligendi omnis voluptate nihil voluptatibus do...  ...

       Proxy Information  Firewall Logs  IDS/IPS Alerts  Log Source  Year  \
0                      1              1               0           0  2023
1                      0              1               0           1  2020
2                      1              1               1           1  2022
```

Fig. 1 Information related to the dataset

This figure gives a general about the data set which ranges from Timestamp and Source IP Address in the format of TEXT, then it moves to Protocol and Traffic Type in the format of INTEGER. It covers the structure, data types and examples of network traffic details, for instance, port-related details, payload details, and logs source details.



```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 40000 entries, 0 to 39999
Data columns (total 25 columns):
 #   Column                Non-Null Count  Dtype
---  ------                --------------  -----
 0   Timestamp             40000 non-null  object
 1   Source IP Address     40000 non-null  object
 2   Destination IP Address 40000 non-null  object
 3   Source Port           40000 non-null  int64
 4   Destination Port      40000 non-null  int64
 5   Protocol              40000 non-null  object
 6   Packet Length         40000 non-null  int64
 7   Packet Type           40000 non-null  object
 8   Traffic Type          40000 non-null  object
 9   Payload Data          40000 non-null  object
 10  Malware Indicators    20000 non-null  object
 11  Anomaly Scores        40000 non-null  float64
 12  Alerts/Warnings       19933 non-null  object
 13  Attack Type           40000 non-null  object
 14  Attack Signature      40000 non-null  object
 15  Action Taken          40000 non-null  object
 16  Severity Level        40000 non-null  object
 17  User Information      40000 non-null  object
 18  Device Information    40000 non-null  object
 19  Network Segment       40000 non-null  object
 20  Geo-location Data     40000 non-null  object
 21  Proxy Information     20149 non-null  object
 22  Firewall Logs         20039 non-null  object
 23  IDS/IPS Alerts        19950 non-null  object
 24  Log Source            40000 non-null  object
dtypes: float64(1), int64(3), object(21)
memory usage: 7.6+ MB
None
```

Fig. 3 Datatype checking

This figure shows the hierarchical breakdown of the dataset where there are 25 columns with 40,000 entries. It displays data types as an object, int64, float64, non-null values and memory taken by each variable [5]. Notable features comprise the Timestamp, Source IP Address, Anomaly Scores and Log Source for net traffic data analysis.

	Source Port	Destination Port	Packet Length	Anomaly Scores
count	40000.000000	40000.000000	40000.000000	40000.000000
mean	32970.356450	33150.868650	781.452725	50.113473
std	18560.425604	18574.668842	416.044192	28.853598
min	1027.000000	1024.000000	64.000000	0.000000
25%	16850.750000	17094.750000	420.000000	25.150000
50%	32856.000000	33004.500000	782.000000	50.345000
75%	48928.250000	49287.000000	1143.000000	75.030000
max	65530.000000	65535.000000	1500.000000	100.000000

Fig. 4 Summary Statistics

This figure shows basic statistical measures of the numerical columns under study, which include Source Port, Destination Port, Packet Length, and Anomaly Scores. The things that can be learned include mean value, standard deviations and range [6]. It underlines fluctuation in the packet size and the anomaly indices helping in anomaly identification and flow pattern study.

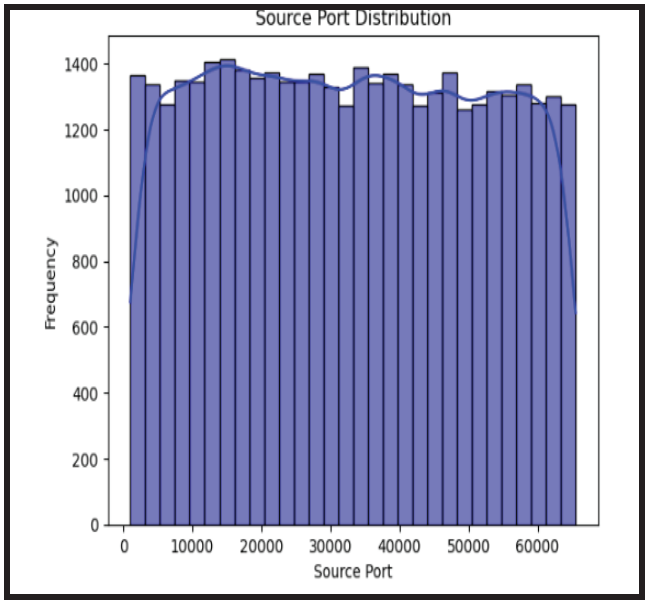


Fig. 5 Source Port Distribution

This bar chart illustrates the number distribution of the source ports of the dataset. Hypothesized by the near absence of a distinct peak which would have pointed towards a particular source port, the calorigram provides scope for uniformity which translates to no concentrated source of traffic in the network [7].

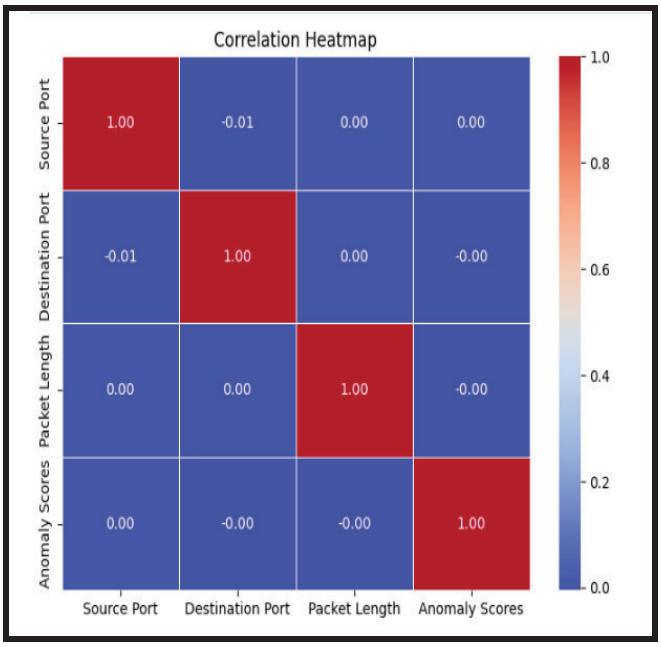


Fig. 6 Correlation Heatmap

This heatmap reflects the interdependency of the numerical values such as Source Port, Destination Port, Packet Length as well as Anomaly scores [8]. The diagonal line shows the ideal level of self-correlation, equal to 1.0, while values low near the diagonal represent low correlation coefficients between the variables, implying that the variables in the model are independent of each other.

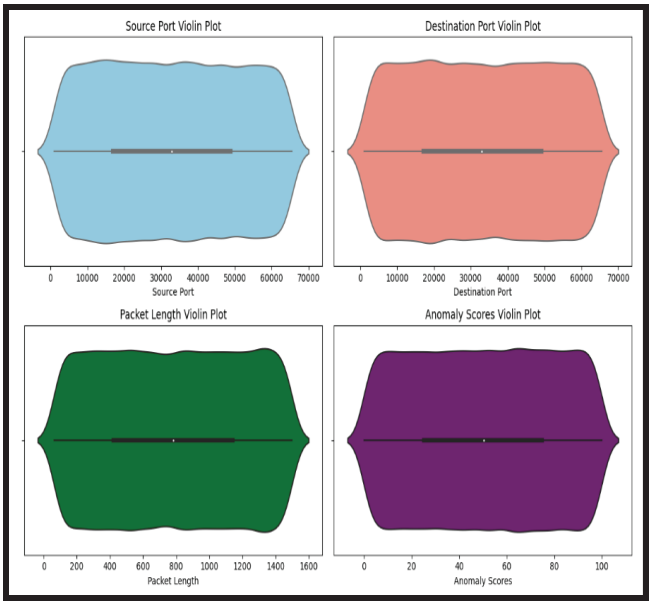


Fig. 7 Violine Plot for displaying Cyber Threats

The violin plots show how Source Port, Destination Port, Packet Length and Anomaly Scores are distributed and dense [9]. Both plots are used to demonstrate the dispersion and distribution of values that allow to detection of outliers or shifts connected to possible cyber threats in network traffic patterns.

```
Index(['Timestamp', 'Source IP Address', 'Destination IP Address', 'Protocol',
       'Packet Type', 'Traffic Type', 'Payload Data', 'Malware Indicators',
       'Alerts/Warnings', 'Attack Type', 'Attack Signature', 'Action Taken',
       'Severity Level', 'User Information', 'Device Information',
       'Network Segment', 'Geo-location Data', 'Proxy Information',
       'Firewall Logs', 'IDS/IPS Alerts', 'Log Source'],
      dtype='object')
```

Fig. 8 Displaying Indexes

This figure displays column headings that belong to the defined dataset they include Timestamp, Source IP Address, Traffic Type, and Attack Signature [10]. This gives an introduction to the various analyses one can perform stressing the availability of several important fields for the network defense against cyber threats.

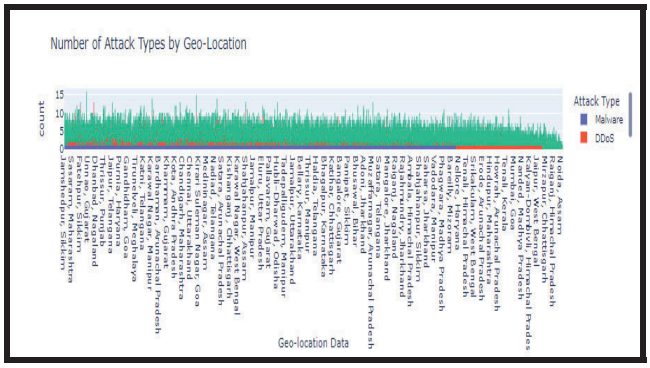


Fig. 9 Displaying the number of attack types by Geo-Location

This bar chart analyses the types of attacks for different geographical locations including Malware and DDoS [11]. This map shows the numerous and varied attacks that occur daily or weekly around the globe, underlining the need for geographic specificity concerning the threat.

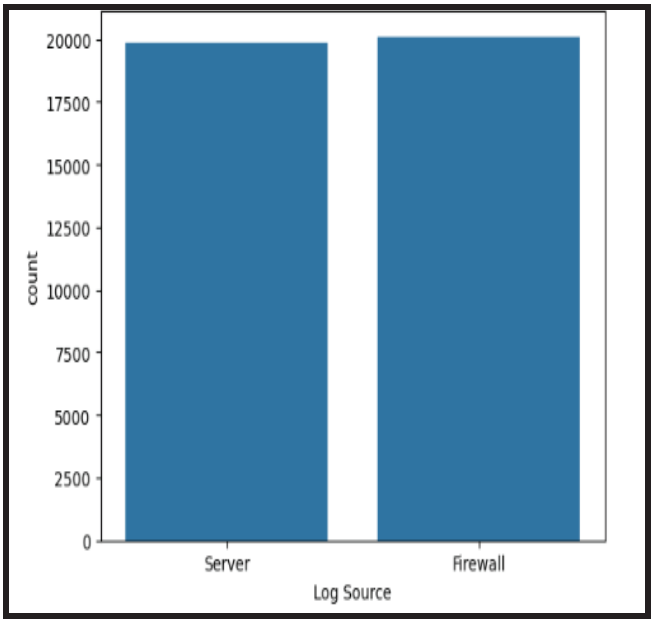


Fig. 10 Displaying Log Sources

This fair bar chart displays the number of server and firewall logs in a given timeframe. We received an almost equal number of logs, with around 20,000 logs from each source [12]. This means that to get maximum control and optimal performance, the monitoring is distributed in such a manner that it covers all areas of the network from multiple perspectives.

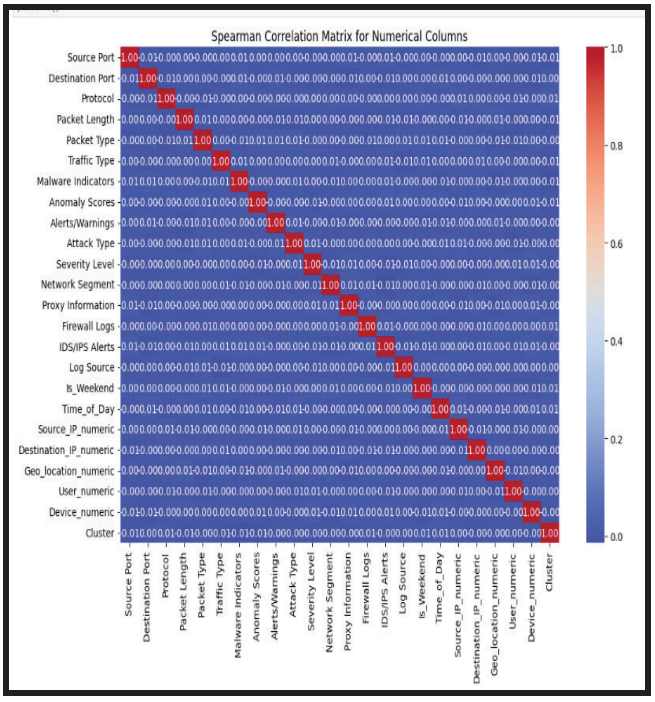


Fig. 11 Spearman Correlation matrix for Numerical Columns

Relative to this matrix, Spearman correlation coefficients between numerical features are presented. Diagonal values are equal to 1 which indicates strong self-correlation; the rest values are either weak or negligible, showing little or no correlation between two variables [13]. This analysis shows feature independence and helps narrow models by choosing non-redundant, effective features for cybersecurity study.

Cluster	Source_IP_numeric	Destination_IP_numeric	Geo_location_numeric
0	-0.015079	0.007214	-0.000573
1	-0.007199	-0.009027	0.007693
2	0.021539	0.008355	-0.006274
3	0.007450	0.004050	-0.000428
4	-0.006286	-0.010293	-0.000302

Cluster	User_numeric	Device_numeric
0	-0.003911	0.007474
1	-0.006637	0.026449
2	0.013954	-0.037650
3	0.000128	-0.001885
4	-0.003497	0.005729

Cluster	Payload Data Numeric
0	573640029406640880690641146696835849870956458 9...
1	341903445232702468825045371562450742961733346 1...
2	104139646914098495901059180250499256372973841 1...
3	113026409147606507647380579354186120773122827 6...
4	809659083148419401659918568829892832871428249 5...

Fig. 12 Displaying the clustering of cyber threats

This figure illustrates the result of clustering for numerical attributes such as Source_IP_numeric, Geo_location_numeric, and Payload Data Numeric [14]. These clusters (0 to 4) are different combinations of similar cyber threat characteristics that are made to understand patterns and separate behaviours for further inspection and threat management plans.

TABLE I. KEY FINDINGS OF THE STUDY

Key Aspects	Key Findings
Blockchain benefits	Blockchain enables decentralized, transparent, and immutable data transactions improving the resilience of cybersecurity.
Cybersecurity Applications	It is effective in protecting against cyber threats like identity theft, DDoS attacks, unauthorized access, and potential data breaches.
Identity management	Blockchain ensures a decentralized and self-sovereign identity system ensuring significant data control and privacy for users.
Data Exchange	Smart contracts facilitate a tamper-proof and secure data exchange without intermediaries.
Key limitations	Key challenges include higher energy usage, scalability issues, and the requirement of efficient consensus models like BFT and PoS.

V. CONCLUSIONS

Blockchain innovates cybersecurity by guaranteeing protected and clear data transfer while conferencing the privacy component. This report takes cognizance of its applicability in reducing cyber threats and enhancing the robustness of digital systems. While there is still a question as to whether blockchain's scalability can be solved while the technology advances on its current path, blockchain has the potential to offer the protection needed for data in a world that is becoming further connected.

REFERENCES

[1] Abdelwahed, I.M., Ramadan, N. and Hefny, H.A., 2020. Cybersecurity risks of blockchain technology. International Journal of Computer Applications, 177(42), pp.8-14.

[2] Alshehri, M., 2023. Blockchain-assisted cyber security in medical things using artificial intelligence. Electron. Res. Arch, 31(2), pp.708-728.

[3] Deshmukh, A., Sreenath, N., Tyagi, A.K. and Abhichandan, U.V.E., 2022, January. Blockchain enabled cyber security: A comprehensive survey. In 2022 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[4] Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P. and Alhelou, H.H., 2021. Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, pp.29429-29440.

[5] He, S., Ficke, E., Pritom, M.M.A., Chen, H., Tang, Q., Chen, Q., Pendleton, M., Njilla, L. and Xu, S., 2022. Blockchain-based automated and robust cyber security management. Journal of Parallel and Distributed Computing, 163, pp.62-82.

[6] Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H., 2023. Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), p.83.

[7] Sriram, V.P., Sanyal, S., Laddunuri, M.M., Subramanian, M., Bose, V., Booshan, B., Shivaram, C., Bettaswamy, M., Booshan, S. and Thangam, D., 2023. Enhancing Cybersecurity Through Blockchain Technology. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 208-224). IGI Global.

[8] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C. and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), p.127.

[9] Ali, A., Rahim, H.A., Pasha, M.F., Dowsley, R., Masud, M., Ali, J. and Baz, M., 2021. Security, privacy, and reliability in digital healthcare systems using blockchain. *Electronics*, *10*(16), p.2034.

[10] Zubaydi, H.D., Varga, P. and Molnár, S., 2023. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. *Sensors*, *23*(2), p.788.

[11] Elisa, N., Yang, L., Chao, F., Naik, N. and Boongoen, T., 2023. A secure and privacy-preserving e-government framework using blockchain and artificial immunity. *IEEE Access*, *11*, pp.8773-8789.

[12] Liu, M., Yeoh, W., Jiang, F. and Choo, K.K.R., 2022. Blockchain for cybersecurity: systematic literature review and classification. *Journal of Computer Information Systems*, *62*(6), pp.1182-1198.

[13] Tyagi, A.K., 2024. Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications. In *AI and Blockchain Applications in Industrial Robotics* (pp. 171-199). IGI Global.

[14] Ali, A., Al-Rimy, B.A.S., Almazroi, A.A., Alsubaei, F.S., Almazroi, A.A. and Saeed, F., 2023. Securing secrets in cyber-physical systems: A cutting-edge privacy approach with consortium blockchain. *Sensors*, *23*(16), p.7162.