ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2023.0456

ANALYSIS OF ONLINE INTRUSION DETECTION MODELS TO INCORPORATE SECURED DIGITAL CASH TRANSACTION IN MOBILE SMART SYSTEMS

R. Bhuvaneswari[1], V. Vasanthi[2], M. Paul Arokiadass Jerald[3] and I. Benjamin Franklin[4]
[1,3]Department of Computer Science, Periyar Arts College, India
[2]Department of Computer Science, Dharmapuram Gnanambigai Government Arts College for Women, India
[4]PG Department of Computer Application, St. Joseph's College of Arts and Science, Cuddalore, India

Abstract

The major Objective of this research paper is to design the Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID) for assessing Intrusion Detection (ID) techniques and evaluating ID parameters that has to be rectified for enhancing the security of Digital Cash Transactions in Mobile Smart devices. The Research examined the Intrusion Detection dataset with 41 predictive features and 1 class feature for evaluating prediction in its novel form. The Framework was examined in WEKA with RapidMiner for analysis. The Results of classifiers Decision Table (98.7%), Random Forest Tree (99.79%), AdaBoost (94.37%), CART Model (99.61%), LazyIBK (99.44%), Naïve Bayesian (89.66%) signified that Smart devices security in Digi cash transactions could be predicted with refinement of data during transaction as deployed in this research work. The cluster analysis again conformed that num_root, su_attempted and num_compromised were the three parameters predominantly used for intrusions in the network and has to be addressed in the model.

Keywords:

Intrusion Detection System, Network Security, Intrusion Detection Parameters, Digital Cash Transactions, Mobile Smart Systems

1. INTRODUCTION

India is regarded as one of the best nations thriving best in global Digital Economy as directed by the Prime Minister of India. In recent survey, it was found in 2022, around 70 billion transactions [1] were completed by people of India. It was a steady increase from 44 billion in 2021. Various digital payment schemes like Gpay, Paytm and Phonepe has been predominantly in practice among the millions of people. Government also focused on the Unified Payment National Payments Corporation of India (NPCI) to encourage cashless transaction among the people. Various countries have accepted payment schemes [2] available in India like RuPay and UPI as a gateway for carrying out their regular transactions. The first one to accept Indian mode of online gateway was Nepal followed by several countries like Singapore, Bhutan, UAE, France etc. The Global payment system has been increasing [3] since 2018 after demonetisation in 2016 to gain trust among the customers including business people, government officials and all the common people. It was recently mentioned by Prime minister of India that every household will be given with cashless transactions in the future. Hence it is highly significant that the security of the system [4] has to be tightened and made securely available for the masses. This is because with inception of any new technology or change, the problems also tend to seek into the system. Same way, the intruders have changed their way of stealing money from physical snatching to online intrusion [5] and money cheat with the knowledge and support of the systems. Thus, a secure platform is required to manipulate the system and bring solution to the problem of handling secure transactions in the future. This is the problem addressed in the research study. The major Objective of this research paper is to design the Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID) for assessing Intrusion Detection (ID) techniques and evaluating ID parameters that has to be rectified for enhancing the security of Digital Cash Transactions in Mobile Smart devices. Various Reearch Questions were pondered to determine the purpose of the research and its relevant outcomes. The substantial analysis and experiments were expected to be performed to determine that there is significant relationship between the selection of relevant parameters in predicting the intrusion during digi cash transactions in smart devices. The scope is applied among mobile smart devices to enhance security of digital cash transactions carried out by people using applications like Gpay, UPI etc. This analysis would ponder to the needs of the futuristic needs of the masses of people in bring quality solution to the problem of being afraid to make transactions in all public places.

2. RELATED WORKS

The research work encompasses few of the earlier works completed by different researchers to promote secured cashless transactions in the digital communications. Lee, H., and Hong, D., [6] focused on the inception of blockchain technology to improve the quality of security in cashless digital transactions. The major idea was to reduce the financial crisis among the organisations due to theft of transactions in online mode. Nandal, N., et.al. [7] analysed the importance of global technology in bringing secured e-transactions for the future. The author believed that such secure transaction would bring sustainable economy for the future. Also, Digital Signature Authentication Cryptosystem was discussed by Islam, A., et.al. [8] to encourage stable E-cash flow in commercial and markets from the customers and investors. The cashless India was dreamt with reliable security by Aggarwal, K., et. al. [9] for better enhancement of finance and business. A secure wallet creation was developed by Igboanusi, I. S., et.al. [10] to bring both offline and online transaction among the common people to grow the number of transactions.

Alupotha, J., et.al. [11] concentrated on the quality of transactions with cryptocurrency using Aggregable and confidential transactions among the business people. Also, this increased the efficiency of Quantum-Safe Cryptocurrencies. Ahamed, S., et.al. [12] discussed on the decentralised security systems on the basis of Blockchain technologies to bring easy payment system for the cash transactions. There is a potential warning for all the cash transactions as suggested by Prasad, E., [13] as it was mentioned that cash would become obsolete in the future and complete cashless transaction will occur among all the people in America. Raj, P. V. R. P., et. al. [14] also suggested that

e-cash transactions would dominate the cash and credit payments using supply chain and block chain enabled security systems. Abad-Segura, E., et. al. [15] initially suggested that blockchain would be highly efficient for securing the accounting process in any financial organisation.

A background study on some of the payment systems followed in India and their Intrusion problems are studied:

USSD Payment: Unstructured Supplementary Service Data (USSD) [16] had reached a wider mass to make payments in digital mode. This could be easily made using a common code *99# without any internet connection. It is very simple and easy to use system of payment. However, the intruder could easily make payment if the mobile was stolen and passcode being released. **Banking Cards:** Banking cards included debit and credit cards that are used by customers with the support of the banks being the chief authenticator [17] and issuer of the cards. Earlier there was an intruder problem to steal the password or pin number. Nowadays, it is verified with One time Password and bring security in transactions. But when they use it in ATM or with the merchant in any shop, it may be intruded in the network arena using wireless scanners or jammers. **UPI payments:** This Unified Payments Interface (UPI) being the extensively used interface [18] is capable of bringing all types of transactions in one area to make digital transaction easier for common people. This works in all smart devices. Hence it could be hacked and intruded when not being taken care of by the user. The links of this mobile application and the customer bank account could be disclosed as well when it is on the control of the intruder. **AEPS Payment System:** Aadhaar Enabled Payment System (AEPS) was newly introduced to link the aadhar card of India to the bank accounts and transactions [19] to reduce the effect of black money in the Indian economy similar to smart card in United states. However, if the intruder comes to know about the Aadhar number, the entire system would come in control of the hacker and money could be lost. **Mobile Wallets:** Mobile wallets represented digital form [20] of the exact physical money being placed in the wallet. The user can add money as and when required for carrying out their regular transactions. However, this wallet could be passively monitored by intruder using brutal force method to know the spending ability of the person and work accordingly to hack into the main bank account in future. **PoS payment system:** PoS(Point of Sale) is predominantly used by business people to carry out their billings. This works wireless and can be easily transacted [21] when the cash is brought closer to the system. It is very easy for intruder to bring any hacking application closer to the PoS machine and corrupt the transactions as transaction may be left incomplete in many cases.

Internet Banking: Internet banking is the oldest and highest mode of operation preferred by professionals and businessmen using their laptops [22] and tablets rather than other smart devices. It is performed by logging into their system and handling huge transactions by the user. Already many intrusions like trafficking and active monitoring, masquerade was a threat to this type of cash transaction system. **Mobile Banking:** Mobile banking is the recent innovation from banks to give an application to the user in the mobile platforms [23]. The user can perform transaction without any common interface to complete their transactions. However, if the intruder could hack into the bank system, the user with the mobile application will also get affected with the problem subsequently without any prior information from banks.

Thus, for all the mode of payment systems available in the online modes, there is an Intrusion problem associated with it. Hence, a, in depth analysis was required to identify the best-known threat for the problem.

3. MATERIALS AND METHODS

Digital transactions have significant improvement by gaining trust among the users from time to time. However, the intrusion has always been a problem that need to be addressed for promoting more enhanced security thereby claiming more interested people and high level of transactions every day. To analyse and understand the type of intrusions in the digital transactions, a dataset was selected from secondary source and examined in the research. The major Objective of this research paper is to design the Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID) for assessing Intrusion Detection (ID) techniques and evaluating ID parameters that has to be rectified for enhancing the security of Digital Cash Transactions in Mobile Smart devices. The Architectural framework of the proposed model comprised of three major stages.

- Feature Analysis
- Classifier Analysis and
- Intrusion Analysis

In Feature Analysis, the training set has been analysed for initial preprocessing with error analysis. After removal of errors in preprocessing, the parameters were tested and the feature analysis process is completed. This process ensures that the right features without errors are selected for predictions. After feature analysis, the best relevant features were selected for training with the classifiers.

In Classifier Analysis, the formed best features set is trained and evaluated with five classifiers including Decision Table, Random Forest Tree, AdaBoost, CART Model, LazyIBK, Naïve Bayesian were tested to find relevant outcomes as evaluation parameters like Correctly Classified Instances (Accuracy), Incorrectly Classified Instances (Error Rate), Kappa statistic, Mean absolute error, Root mean squared error, Relative absolute error and Root relative squared error to indicate the correctness of the classification. The trained model has been used as testing set for detecting intrusions in digital transactions.

During, the Intrusion Analysis, the testing set is loaded into the RapidMiner tool using the design part of the implementation containing normalization and cluster analysis with k-means clustering is performed as part of the novel Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID) to determine the anomalies' part and the normal part during the intrusion detection. The outcomes were expected to be tested and analysed with the proposed model as shown in Fig.1.

As determined in Fig.1., the Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID) has significantly been expected to identify the potential needs of recent Digital Cash Transactions and its flaws to be eradicated to identify the potential anomalies or intrusions and enhance security of network transactions.

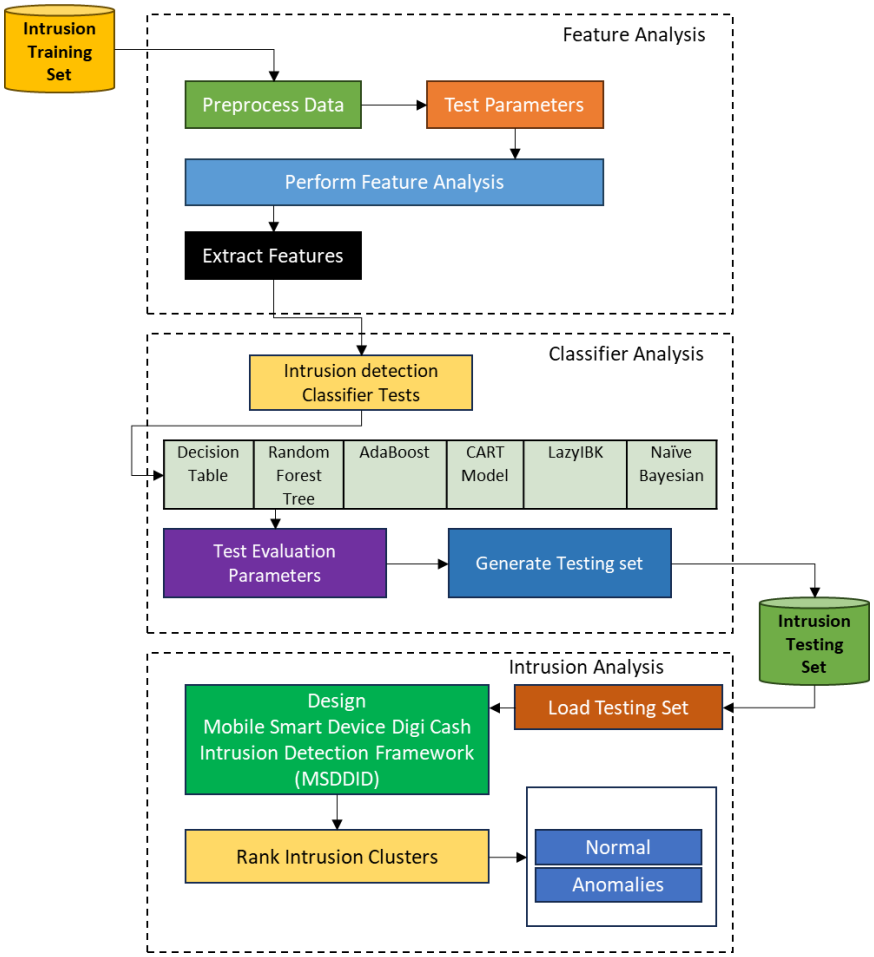

Fig.1. Proposed Novel Mobile Smart Device Digi Cash Intrusion Detection Framework (MSDDID)

Table.1. Parameters of the Intrusion Detection dataset and its information

Sl. No.	Name of the Feature	Purpose	Max. Value	Min. Value
1	duration	Duration of Transmission	1	100
2	protocol_type	Type of Protocol	TCP/IP	IMCP
3	service	Type of Service	ftp_data	private
4	flag	Flag Set for Transaction	SF REJ	S0
5	src_bytes	Source Bytes	0	491
6	dst_bytes	Destination Bytes	0	0
7	land	Land	0	0
8	wrong_fragment	No. of Wrong fragments	0	0
9	urgent	Urgent data sent	0	0
10	hot	Hot data sent	0	0
11	num_failed_logins	No. of failed Logins	0	0
12	logged_in	Logged In Status	0	0
13	num_compromised	No Compromised	0	0
14	root_shell	No of Shells in the root directory	0	0
15	su_attempted	Su root command attempts	0	0
16	num_root	Number of roots	0	0
17	num_file_creations	Number of file creations	0	0
18	num_shells	Number of shells	0	0

19	num_access_files	Number of Access files	0	0
20	num_outbound_cmds	Number of Outbound Commands	0	0
21	is_host_login	Whether host Logged in?	0	0
22	is_guest_login	Whether guest Logged in?	0	0
23	count	Number of transactions	2	38
24	srv_count	Number of transactions to same service	2	9
25	serror_rate	Number of transactions with error in S1, S2, S3, S4	0	1
26	srv_serror_rate	Number of transactions from same service to error	0	1
27	rerror_rate	Number of error transactions to REJ	0	0
28	srv_rerror_rate	Number of transactions to same connection to REJ error	0	0
29	same_srv_rate	Similar errors at a particular time	0.24	1
30	diff_srv_rate	Different errors at a particular time	0	0.11
31	srv_diff_host_rate	Same source to different host transaction rate	0	0
32	dst_host_count	Destination host count	150	255
33	dst_host_srv_count	Destination host to server count	25	49
34	dst_host_same_srv_rate	Destination to host at same level	0.17	0.19
35	dst_host_diff_srv_rate	Destination to host at different rate	0.03	0.03
36	dst_host_same_src_port_rate	Destination to host with same source port rate	0.01	0.17
37	dst_host_srv_diff_host_rate	Destination to host with different host rate	0	0
38	dst_host_serror_rate	Destination to host error rate	0	1
39	dst_host_srv_serror_rate	Destination to host with same connection error rate	0	1
40	dst_host_rerror_rate	Destination to host REJ error rate	0	0.05
41	dst_host_srv_rerror_rate	Destination to host same connection REJ error rate	0	0
42	class	Type of Intrusion detection in the Online Transaction	Normal	Anomaly

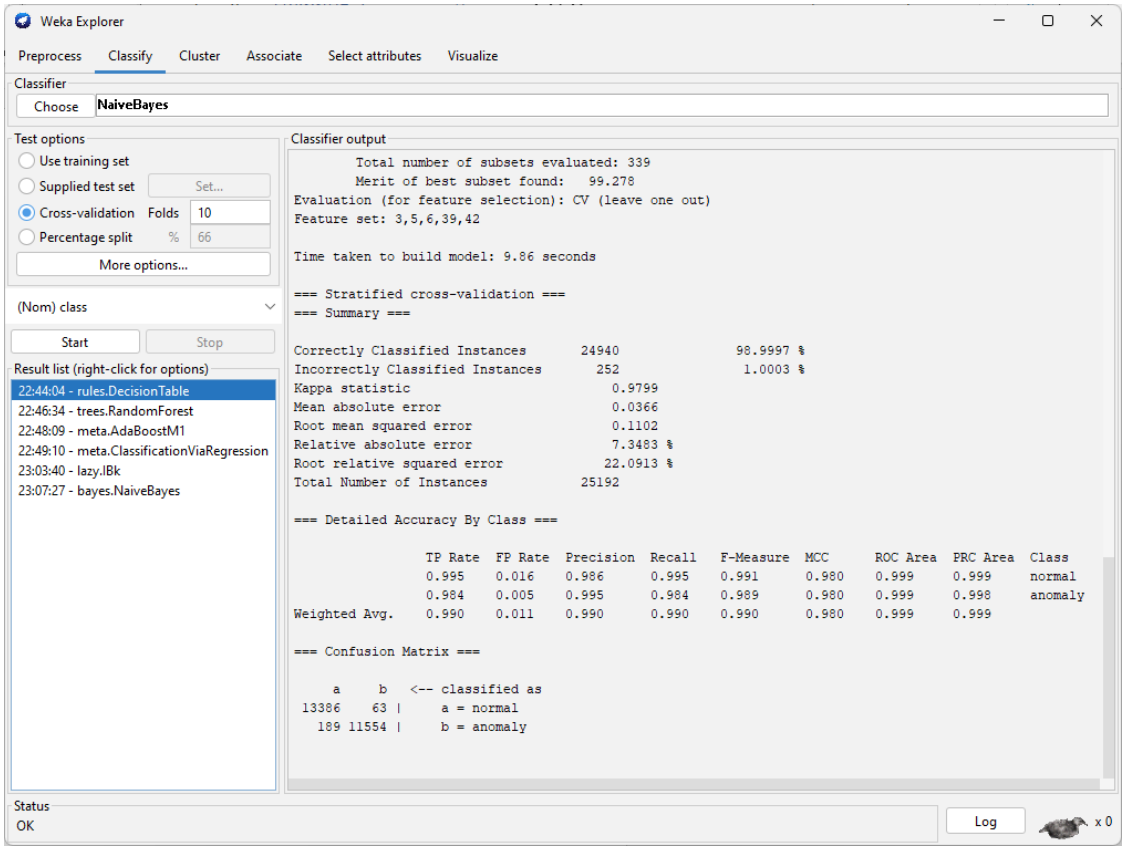

Fig.2. Examining the Intrusion Detection dataset in WEKA tool for testing performance

3.1 DATASET ANALYSIS

The Intrusion Detection Analysis (IDA) dataset was prepared and shared by military network environment in US Air Force LAN. The dataset consisted of the training and the testing set where the features [5] were ordered based on the number of intrusions simulated in the network managed by the military in Local Area Network (LAN). Also, the analysis of Transmission Control Protocol and Internet Protocol (TCP/IP) packets was presented with different parameters. The connection of the starting bit of the TCP/IP packet and the targeted IP packets were presented in the dataset. Each connection of the TCP packets were labelled and also the flow of data from source to destination was recorded as shown in Table.1.

It is evident from Table.1. that there was 41 predictive attributes and 1 class attribute with values 0-Normal and 1-Anomaly to indicate that there was good normal transaction or anomaly-based transaction in the network. The features were both qualitative and quantitative in their behaviour. Hence an examination was required for preparing the data without errors

3.2 DATA PREPARATION AND EXAMINATION

The Intrusion Detection dataset was analysed and examined using WEKA tool to evaluate the quality of input features for the future predictions. The training set in excel form was loaded into WEKA and tested in the explorer with six different types of algorithms including Decision Table (DT), Random Forest Tree (RFT), AdaBoost, Classification and Regression Technique (CART), Lazy Instance based Learning Model and Naïve Bayesian model respectively as shown in Fig.2. The classifier results of five different models were obtained as indicated in a sample result with WEKA tool shown in Fig.2.

4. IMPLEMENTATION

As shown in Fig.3., the clusters were predominantly correctly classified with only few of the data were wrongly classified. The prepared dataset was implemented in Rapid miner using the design of data process. The Model was also proposed based on the different stages as shown in Fig.4.

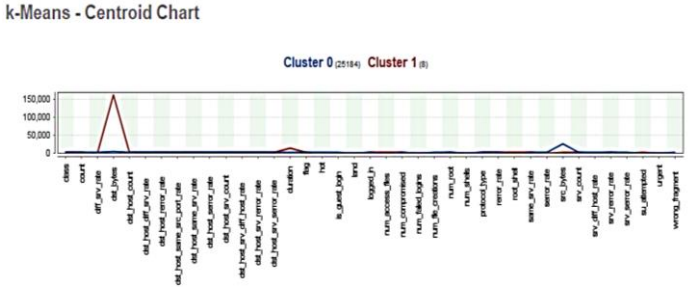

Fig.3. Cluster formation for Intrusion Detection dataset after examination in rapid miner

The dataset was then analysed using RapidMiner Studio to identify the errors in the system. The normal transactions and Anomaly transactions were grouped together using cluster analysis. The K-Means model using the centroid 'K' for grouping cluster-0 as best formed data and cluster-1 as wrongly classified data is performed. The cluster formation based on the centroids are given in Fig.3.

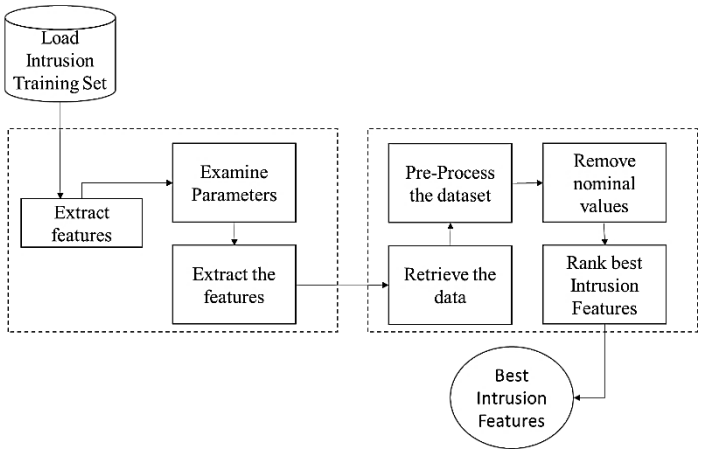

Fig.4(a). Intrusion detection parameter analysis model

As shown in Fig.4., various stages were implemented starting from retrieval of data and pre-processing using relevant methods of the network security. Later, the text data and numeric data were segregated and formed as clusters for further analysis. Later, the prediction was initiated with 10 cross folds as it was done in WEKA and unwanted parameters were removed at the end of the predictive analytics process as shown in Fig.4.

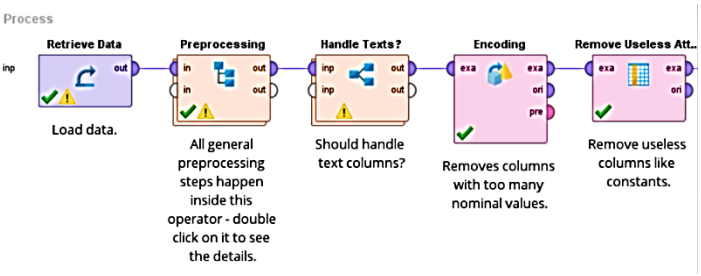

Fig.4(b). Intrusion detection parameter analysis model

As shown in Fig.5., the design was performed and the clusters were formed as cluster-0 and cluster-1 as shown in Table.2.

Table.2. The centroid values identified in cluster 0 and 1 after k-mean analysis

Sl. No.	Feature	Cluster 0	Cluster 1
1	class	1	1
2	count	84.618	1
3	diff_srv_rate	0.062	0
4	dst_bytes	3441.791	161068
5	dst_host_count	182.555	111.375
6	dst_host_diff_srv_rate	0.083	0.116
7	dst_host_rerror_rate	0.118	0.026
8	dst_host_same_src_port_rate	0.147	0.042
9	dst_host_same_srv_rate	0.52	0.228
10	dst_host_serror_rate	0.286	0.152
11	dst_host_srv_count	115.093	19.5
12	dst_host_srv_diff_host_rate	0.032	0.063

13	dst_host_srv_rerror_rate	0.119	0.079
14	dst_host_srv_serror_rate	0.28	0.146
15	duration	300.782	13754.38
16	flag	9	9
17	hot	0.198	0
18	is_guest_login	0.009	0
19	land	0	0
20	logged_in	0.395	1
21	num_access_files	0.003	4
22	num_compromised	0.059	532.25
23	num_failed_logins	0.001	0
24	num_file_creations	0.015	0
25	num_root	0.062	590.875
26	num_shells	0	0
27	protocol_type	1	1
28	rerror_rate	0.119	0.125
29	root_shell	0.001	1
30	same_srv_rate	0.66	1
31	serror_rate	0.286	0
32	src_bytes	24338.08	863.625
33	srv_count	27.707	1
34	srv_diff_host_rate	0.096	0
35	srv_rerror_rate	0.12	0.125
36	srv_serror_rate	0.284	0
37	su_attempted	0.001	2
38	urgent	0	0
39	wrong_fragment	0.024	0

The clusters formed in Table.2. after examination was analysed using rapidminer model to that out of 25,192 records 25,184 data were correctly classified for prediction and only 8 records were wrongly classified for prediction as shown in Fig.6.

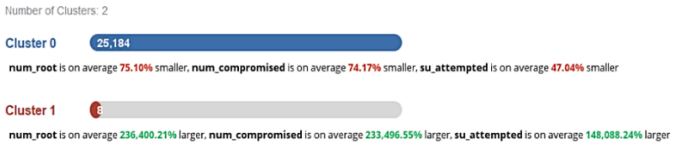

Fig.6. Classification of Cluster-0 and Cluster-1 after implementation with the model

As shown in Fig.6. the cluster-0 with correctly classified values showed that 75.10% of the intrusion was found in num_root indicating root directory, 74.17% indicating compromised intrusions and 47.04% indicating 'su' command errors respectively. Thus, the clusters indicated that maximum intrusions were possible in the root area of the digital transactions. The wrongly classified cluster-1 also showed the same parameters as intrusion problems in a smart system.

5. RESULT AND DISCUSSION

The implementation was completed in two phases from WEKA for examination and RapidMiner for Analysis on the highest level of intrusions that might occur in the smart systems. In the initial stage, the classifiers were used to test the intrusion detection dataset and the results of prediction was summarised in Table.3.

It was evident from Table.3. that the correctly classified values for the Intrusion Detection dataset have been at an average range of 90% to 99% like the identification in RapidMiner predictions. The incorrectly classified values were very less. Hence the prediction accuracy would be high to analyse and test the intrusion parameters in this dataset. The positive predictions like kappa statistic (KS) were found positive with around 0.9 whereas the negative predictions like Mean absolute error (MAE), Root mean squared error (RMSE), Relative absolute error (RAE) and Root relative squared error (RRSE) are found to show reduced values relatively to positive values.

The formed results were then compared and tested with RapidMiner Analysis model to detect the percentage of anomalies and normal transactions. It was found that 13,449 records had normal transactions without anomalies accounting to 53.39% and

11,743 records had anomaly transactions with anomalies of 46.61% percent respectively. The class analysis of the expected results is shown in Fig.7.

As shown in Fig.7., the evaluation of dataset after feature extraction has resulted in better anomaly detection indicating intrusion detection with 46.61% and normal status with 53.39% respectively. This result was in accordance with the outcomes achieved from intrusion detections achieved manually. The cluster analysis again confirmed that num_root, su_attempted and num_compromised were the three parameters predominantly used for intrusions in the network and must be addressed in the model.

Table.3. Examination results of tested intrusion detection dataset with classifiers

Benchmark Threshold achievements (90% to 99%)	**Decision Table**	**Random Forest Tree**	**Ada Boost**	**CART Model**	**Lazy IBK**	**Naïve Bayesian**
Correctly Classified Instances	98.7%	99.79%	94.37%	99.61%	99.44%	89.66%
Incorrectly Classified Instances	1.3%	0.21%	5.63%	0.39%	0.56%	10.34%
KS	0.9799	0.9957	0.8866	0.9921	0.9888	0.792
MAE	0.0366	0.0066	0.0796	0.0105	0.0056	0.1028
RMSE	0.1102	0.0443	0.1949	0.0621	0.0748	0.3143
RAE	7.34%	1.32%	16.00%	2.11%	1.13%	20.65%
RRSE	22.09%	8.88%	39.07%	12.4%	14.9%	62.99%

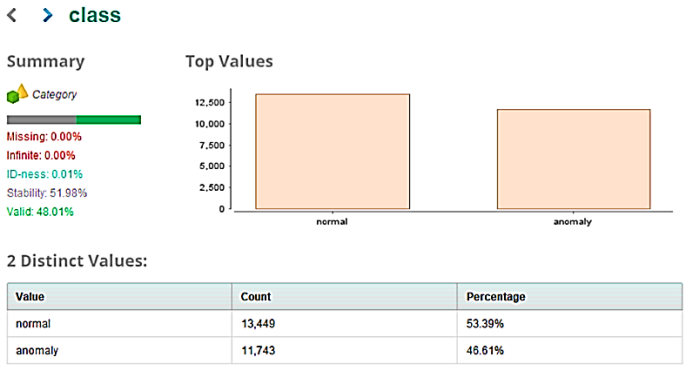

Fig.7. Class feature examination to analyse expected outcomes of intrusion

The attack on the root is a serious problem as it may totally shut down the entire system. Thus, it is the highest level of intrusion problem to be rectified in the beginning of designing the security system. The 'su'or Switch User command in Linux is another important process where the intrusion normally occurs as someone might impersonate or switch to hacked profiles. Hence it also has to be protected in the beginning stage itself.

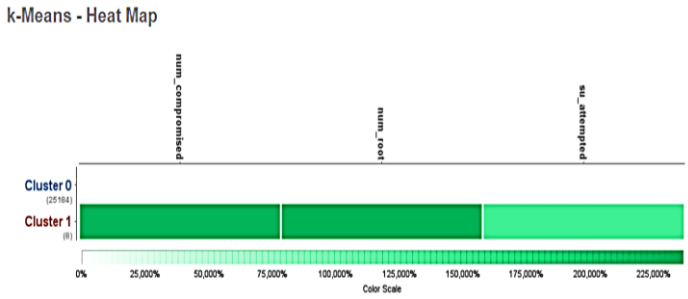

Fig.8. Identification of best intrusion problems to be addressed based on analysis of dataset

The compromised number of connections during any transaction is also identified as one of the important intrusion problems as compromised connections might contain intruder connection for hacking into the system. The best intrusions that might occur in the network security for smart systems during digital cash transactions and results are identified and presented in Fig.8. As shown in Fig.8., the k-means analysis showed that root-based intrusions are at maximum level, followed by switch user command and compromise commands. By setting a prevention mechanism for the identified intrusions, the security could be enhanced in the future.

6. CONCLUSION

The research work has shown a method to analyse and examine the type of intrusions in mobile smart devices and the highest-level intrusions were found as root commands, switch user commands and compromise connection commands respectively. The implementation has also found the solution of provide secure cash transaction in mobile smart devices with enhanced security. The research work confirming the parameters could be implemented in wireless devices or body area networks in the near future.

REFERENCES

[1] P.V. Ranjith, S. Kulkarni and A.J. Varma, "A Literature Study of Consumer Perception Towards Digital Payment Mode in India", *Psychology and Education*, Vol. 58, No. 1, pp. 3304-3319, 2021.

[2] K.V. Satya, "Emerging Trends of Digital Transactions Replacing Cash Transactions in India - An Empirical Study", *Future Internet*, Vol. 56, No. 2, pp. 1-12, 2022.

[3] K. Kajol and R. Singh, "Users' Awareness Towards Digital Financial Transactions: A Study Conducted in India", *Proceedings of International Working Conference on Transfer and Diffusion of IT*, pp. 331-345, 2022.

[4] P. Deshmukh and K.S. Thakare, "Digital India Digital Economy using BCT", *International Journal of Advance Scientific Research and Engineering Trends*, Vol. 6, No. 6, pp.1-11, 2021.

[5] V. Mohite, R. Shikhare and P. Sarangdhar, "Digital Payment Saga: Pandemic Impact on ATM Usage in India", Available at https://easychair.org/publications/preprint/XkJR, Accessed at 2021.

[6] H. Lee and D. Hong, "The Tokenization of Space and Cash Out without Debt: Focus on Security Token Offerings using Blockchain Technology", *Journal of the Economic Geographical Society of Korea*, Vol. 24, No. 1, pp. 76-101, 2021.

[7] N. Nandal, K. Mankotia and M.N. Jora, "Investigating Digital Transactions in the Interest of a Sustainable Economy", *International Journal of Modern Agriculture*, Vol. 10, No. 1, pp. 1150-1162, 2021.

[8] A. Islam, J. Nime, S. Hossain and M. Dutta, "An Online E-Cash Scheme with Digital Signature Authentication Cryptosystem", *Proceedings of International Conference on Sustainable Communication Networks and Application*, pp. 29-39, 2021.

[9] K. Aggarwal and D. Paul, "Moving from Cash to Cashless Economy: Toward Digital India", *The Journal of Asian Finance, Economics and Business*, Vol. 8, No. 4, pp. 43-54, 2021.

[10] I.S. Igboanusi, J.M. Lee and D.S. Kim, "Blockchain Side Implementation of Pure Wallet (PW): An Offline Transaction Architecture", *ICT Express*, Vol. 7, No. 3, pp. 327-334, 2021.

[11] J. Alupotha, X. Boyen and M. Mckague, "Aggregable Confidential Transactions for Efficient Quantum-Safe Cryptocurrencies", *IEEE Access*, Vol. 10, pp. 17722-17747, 2022.

[12] S. Ahamed, A. Anjum and M. Biswas, "Bps: Blockchain based Decentralized Secure and Versatile Light Payment System", *Asian Journal of Research in Computer Science*, Vol. 2021, pp. 12-20, 2021.

[13] E. Prasad, "Cash will Soon be Obsolete: Will America be Ready", Available at https://www.nytimes.com/2021/07/22/opinion/cash-digital-currency-central-bank.html, Accessed at 2021.

[14] P.V.R.P. Raj, M. Ramkumar and S. Pratap, "Procurement, Traceability and Advance Cash Credit Payment Transactions in Supply Chain using Blockchain Smart

Contracts", *Computers and Industrial Engineering*, Vol. 167, pp. 1-11, 2022.

[15] E. Abad-Segura and E. Lopez Meneses, "Blockchain Technology for Secure Accounting Management: Research Trends Analysis", *Mathematics*, Vol. 9, No. 14, pp. 1631-1638, 2021.

[16] P. Dayang and A. Hamza, "Using USSD-based Mobile Payment in Context of Low Internet Connection", *International Journal of Wireless Communications and Mobile Computing*, Vol. 9, No. 1, pp. 1-13, 2021.

[17] B. Chaimaa and H. Rachid, "E-banking Overview: Concepts, Challenges and Solutions", *Wireless Personal Communications*, Vol. 117, No. 2, pp. 1059-1078, 2021.

[18] S. Rastogi, C. Panse and V.M. Bhimavarapu, "Unified Payment Interface (UPI): A Digital Innovation and its Impact on Financial Inclusion and Economic Development", *Universal Journal of Accounting and Finance*, Vol. 9, No. 3, pp. 518-530, 2021.

[19] K.M. Siby, "A Study on Consumer Perception of Digital Payment Methods in Times of Covid Pandemic", *International Journal of Scientific Research in Engineering and Management*, Vol. 5, No. 3, pp. 1-12, 2021.

[20] R.K. Gupta, "Adoption of Mobile Wallet Services: An Empirical Analysis", *International Journal of Intellectual Property Management*, Vol. 12, No. 3, pp. 341-353, 2022.

[21] S.N.A. Sulaima and M.N. Almunawar, "The Adoption of Biometric Point-of-Sale Terminal for Payments", *Journal of Science and Technology Policy Management*, Vol. 13, No. 3, pp. 585-605, 2021.

[22] M. Naeem and W. Ozuem, "The Role of Social Media in Internet Banking Transition during COVID-19 Pandemic: Using Multiple Methods and Sources in Qualitative Research", *Journal of Retailing and Consumer Services*, Vol. 60, pp. 102483-102495, 2021.

[23] E.H.M. Payne, J. Peltier and V.A. Barger, "Enhancing the Value Co-Creation Process: Artificial Intelligence and Mobile Banking Service Platforms", *Journal of Research in Interactive Marketing*, Vol. 15, No. 1, pp. 1-9, 2021.

[24] R. Sekhar and K. Thangavel, "A Novel GPU Based Intrusion Detection System using Deep Autoencoder with Fruitfly Optimization", *SN Applied Sciences*, Vol. 3, No. 6, pp. 1-16, 2021.