CYBER HACKING BREACH PREDICTION USING ADVANCED AI MODELS

#1 B AMARNATH REDDY, #2 T PAVANI
#1 ASSISTANT PROFESSOR
#2 MCA SCHOLAR
DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
QIS COLLEGE OF ENGINEERING & TECHNOLOGY
VENGAMUKKAPALEM (V), ONGOLE, PRAKASAM DIST, ANDHRA PRADESH-523272

ABSTRACT

Examining cyber event data sets is a crucial approach for enhancing our comprehension of the evolving threat landscape. This is a somewhat novel research area, and numerous investigations are yet to be conducted. This study presents a statistical analysis of a dataset pertaining to breach incidents during a 12-year period (2005–2017) including cyber hacking operations, including malware attacks. We demonstrate that, contrary to existing literature, both the inter-arrival periods of hacking breach incidents and the sizes of breaches should be described using stochastic processes rather than distributions, as they display autocorrelations. We offer specific stochastic process models to fit the inter-arrival periods and breach sizes, respectively. We additionally demonstrate that these models can forecast the inter-arrival intervals and the breach magnitudes. To gain deeper insights into the evolution of hacker breach incidents, we do both qualitative and quantitative trend studies on the dataset. We derive a collection of cyber security insights, indicating that the frequency of cyber intrusions is indeed growing, yet the severity of their damage remains unchanged.

I. INTRODUCTION

Hacking into a computer involves exploiting its computing system or private network. Data breaches occur when sensitive, confidential, or otherwise protected information is accessed unlawfully by cybercriminals through a computer or network during an attack. They constitute the act of unauthorized intrusion into a network security system for nefarious objectives. Cyber-attacks are assaults executed by cybercriminals utilizing one or more computers or networks. A data breach poses risks of embarrassment, diminished employment prospects, and forfeited economic chances. This is a verified occurrence in which sensitive, confidential information is accessed or disclosed without authorization. Privacy breaches entail risks

such as humiliation, diminished employment prospects, and forfeiture of business chances. Cybercriminals who effectively penetrate data sources and extract sensitive information because data breaches that threaten physical safety and facilitate identity theft. Data breaches can occur physically by accessing computers or networks to obtain local files, or remotely by circumventing network security measures. The latest data breaches have constituted some of the most significant in documented history. Devastating cyber incidents encompass data breaches. According to the Privacy Rights Clearinghouse, since 2005, there have been several breaches of records, amounting to 9,919,228,821. The Identity Theft Resource Center and Cyber Scout recorded 1,093 breaches in 2016, a 40% increase from the 780 breaches in 2015. During the initial half of 2019, data breaches exposed 4.1 billion records. By 2019, there were 1,473 recorded data breaches in the United States, resulting in the exposure of over 164.68 million sensitive records. Over 3,800 breach reports have been released, revealing 4.1 billion records. The rising utilization of digital files and the significant dependence on digital data by organizations and individuals have heightened awareness of data breaches. Since January 2020, around 7.9 billion records have been compromised in data breaches, encompassing credit card numbers, residential addresses, telephone numbers, and other extremely sensitive information.

Devastating cyber incidents encompass data breaches. According to the Privacy Rights Clearinghouse, since 2005, there have been several breaches of records, amounting to 9,919,228,821. The Identity Theft Resource Center and Cyber Scout recorded 1,093 breaches in 2016, a 40% increase from the 780 breaches in 2015.

II. RELATEDWORKS

1. Cyber Risk Prediction via Social Media & CVE Analysis (2019)

Authors:Subroto & Apriyana
Approach:Combines CVE summaries and Twitter chatter, feeding them into ML classifiers and ANN to predict cyber risk, achieving ~96.7% accuracy arxiv.org+4sciencepubco.com+4sersc.org+4.
Merits:High accuracy, timely detection of emerging threats.
Demerits: Relies on labeled data, potential bias from social media noise.

2. Statistical Stochastic Modeling of Breach Events (2020–2023)

Authors: Srinija *et al.*
Approach: Analyzes 12-year breach data, modeling inter-arrival times and breach sizes via stochastic processes (ARMA-GARCH) instead of static distributions .
Merits: Captures temporal dependencies, auto-correlation in breach patterns.
Demerits: Needs long-term historical data, limited to retrospective prediction.

3. Deep Learning for Forecasting Breach Rates (2019)

Authors:Yuan *et al.*
Approach: Uses bi-directional LSTM networks to forecast attack rates across multiple datasets, achieving <5% error for most cases .

Merits: Handles non-linear time-series data; high forecasting accuracy.
Demerits: Performance varies across datasets; LSTMs are computationally intensive.

4. Hybrid ML Framework for Real-Time Breach Prediction (2020)

Authors: Anonymous study in IJET
Approach: Combines SVM, Random Forest, and Neural Networks for real-time anomaly detection in network traffic to proactively predict breaches.
Merits: Ensemble approach improves detection accuracy; supports real-time alerts.
Demerits: Vague dataset descriptions; practical deployment details lacking.

5. Dark Web & Social-Sensor Signals for Enterprise Attack Prediction (2019)

Authors:Sarkar *et al.*
Approach: Mines dark-web forum interactions and social signals (Twitter) for enterprise attack forecasting via network-structure features and supervised models .
Merits: Innovative use of social media and dark-web intelligence; outperforms simple content-based methods.
Demerits: Ground truth labeling is challenging; data collection reliant on select forums.

III. SYSTEMANALYSIS EXISTING SYSTEM

The present study is motivated by several questions that have not been investigated until now, such as: Are data breaches caused by cyber-attacks increasing, decreasing, or stabilizing? A principled answer to this question will give us a clear insight into the overall situation of cyber threats. This question was not answered by previous studies. Specifically, the dataset analyzed in only covered the time span from 2000 to 2008 and does not necessarily contain the breach incidents that are caused by cyber-attacks; the dataset analyzed in [9] is more recent, but contains two kinds of incidents: negligent breaches (i.e., incidents caused by lost, discarded, stolen devices and other reasons) and malicious breaching. Since negligent breaches represent more human errors than cyber-attacks, we do not consider them in the present study. Because the malicious breaches studied in [9] contain four sub-categories: hacking (including malware), insider, payment card fraud, and unknown, this study will focus on the hacking sub-category (called hacking breach dataset thereafter), while noting that the other three sub-categories are interesting on their own and should be analysed separately.Recently, researchers started modelling data breach incidents. Maillart and Sornettestudied the statistical properties of the personal identity losses in the United States between year 2000 and 2008. They found that the number of breach incidents dramatically increases from 2000 to July 2006 but remains stable thereafter. Edwards et al. analyzed a dataset containing 2,253 breach incidents that span over a decade (2005 to 2015). They found that neither the size nor the frequency of data breaches has increased over the years. Wheatley et al., analyzed a dataset that is combined from corresponds to organizational breach incidents between year 2000 and 2015. They

found that the frequency of large breach incidents (i.e., the ones that breach more than 50,000 records) occurring to US firms is independent of time, but the frequency of large breach incidents occurring to non-US firms exhibits an increasing trend.

PROPOSED SYSTEM

In this paper, we make the following three contributions. First, we show that both the hacking breach incident interracial times (reflecting incident frequency) and breach sizes should be modeled by stochastic processes, rather than by distributions. We find that a particular point process can adequately describe the evolution of the hacking breach incidents inter-arrival times and that a particular ARMA-GARCH model can adequately describe the evolution of the hacking breach sizes, where ARMA is acronym for "AutoRegressive and Moving Average" and GARCH is acronym for "Generalized AutoregressiveHeteroskedasticity."We show that these stochastic process models can predict the inter-arrival times and the breach sizes. To the best of our knowledge, this is the first paper showing that stochastic processes, rather than distributions, should be used to model these cyber threat factors. Second, we discover a positive dependence between the incidents inter-arrival times and the breach sizes, and show that this dependence can be adequately described by a particular copula. We also show that when predicting inter-arrival times and breach sizes, it is necessary to consider the dependence; otherwise, the prediction results are not accurate. To the best of our knowledge, this is the first work showing the existence of this dependence and the consequence of ignoring it. Third, we conduct both qualitative and quantitative trend analyses of the cyber hacking breach incidents. We find that the situation is indeed getting worse in terms of the incidents inter-arrival time because hacking breach incidents become more and more frequent, but the situation is stabilizing in terms of the incident breach size, indicating that the damage of individual hacking breach incidents will not get much worse. We hope the present study will inspire more investigations, which can offer deep insights into alternate risk mitigation approaches. Such insights are useful to insurance companies, government agencies, and regulators because they need to deeply understand the nature of data breach risks.

IV.IMPLEMENTATION

MODULES

1. **UPLOAD DATA**

The data resource to database can be uploaded by both administrator and authorized user. The data can be uploaded with key in order to maintain the secrecy of the data that is not released without knowledge of user. The users are authorized based on their details that are shared to admin and admin can authorize each user. Only Authorized users are allowed to access the system and upload or request for files.

2. **ACCESS DETAILS**

The access of data from the database can be given by administrators. Uploaded data are managed by admin and admin is the only person to provide the rights to process the

accessing details and approve or unapproved users based on their details.

3. USER PERMISSIONS

The data from any resources are allowed to access the data with only permission from administrator. Prior to access data, users are allowed by admin to share their data and verify the details which are provided by user. If user is access the data with wrong attempts then, users are blocked accordingly. If user is requested to unblock them, based on the requests and previous activities admin is unblock users.

4. DATA ANALYSIS

Data analyses are done with the help of graph. The collected data are applied to graph in order to get the best analysis and prediction of dataset and given data policies. The dataset can be analyzed through this pictorial representation in order to better understand of the data details.

METHODOLOGY

1. Requirement and Problem Definition

- Identify the need for proactive prediction of cyber hacking breaches to improve organizational security.
- Define objectives:
  ✓ Model historical cyber breach patterns.
  ✓ Predict future breach events using statistical and machine learning techniques.
  ✓ Provide actionable insights to security teams for early intervention.

2. Data Collection

- Gather historical breach data from credible sources such as:
  ✓ Public breach databases (e.g., Privacy Rights Clearinghouse, Verizon DBIR).
  ✓ Dark web monitoring platforms for leaked credentials or breach discussions.
  ✓ Social media platforms (e.g., Twitter) for cyber threat signals.
  ✓ CVE (Common Vulnerabilities and Exposures) databases for vulnerability trends.

3. Data Preprocessing

- Clean and normalize data to handle missing, incomplete, or inconsistent records.
- Perform feature extraction such as:
  ✓ Breach type, industry sector, date of occurrence.
  ✓ Size and severity of breach.
  ✓ Related vulnerabilities or known threat indicators.
- Convert textual data (e.g., social media posts, dark web discussions) into structured features using NLP techniques if applicable.

4. Feature Engineering

- Engineer relevant features to enhance model performance, including:
  ✓ Temporal features (e.g., time since last breach, seasonal patterns).
  ✓ Threat intelligence indicators

(e.g., emerging exploits, leaked data mentions).

✓ Network traffic anomaly scores (if real-time prediction is incorporated).

- Normalize and scale features for consistency.

5. Modeling Approaches

- Implement multiple modeling techniques to capture breach patterns:

✓Statistical Models:

- Time-series analysis (e.g., ARIMA, Poisson models) for breach frequency modeling.
- Stochastic models (e.g., ARMA-GARCH) to capture breach volatility over time.

✓Machine Learning Models:

- Supervised learning (e.g., Random Forest, SVM) to classify breach likelihood.
- Deep learning models (e.g., LSTM) for sequential breach prediction based on time-series data.

✓Hybrid Approaches:

- Combine statistical forecasting with machine learning for improved predictive accuracy.

6. Model Training and Validation

- Split the dataset into training, validation, and testing sets.
- Train models using historical data with proper parameter tuning.
- Validate model performance using:

✓ Classification Metrics: Accuracy, Precision, Recall, F1-score (for breach occurrence prediction).

✓ Time-Series Metrics: RMSE, MAE, MAPE (for breach frequency/severity prediction).

- Perform cross-validation to ensure model robustness.

7. Integration of External Signals (Optional)

- Enhance the model by integrating real-time signals such as:

✓ Dark web discussions related to targeted organizations.

✓ Social media posts indicating exploit discussions or attack claims.

✓ CVE trends for emerging vulnerabilities.

- Use NLP and sentiment analysis to convert these unstructured signals into quantitative features.

8. Breach Prediction and Risk Estimation

- Deploy the trained model to predict:

✓ Likelihood of a cyber-hacking breach in a future time window.

✓ Estimated breach frequency or severity over time.

- Provide risk scores or alerts to security teams for proactive action.

9. Evaluation and Continuous Improvement

- Continuously monitor model performance with newly observed breach data.
- Update models periodically to incorporate evolving attack patterns and threat landscapes.
- Refine feature sets and algorithms based on feedback from security experts.

10. Deployment and Practical Use

- Integrate the prediction system into organizational security operations.
- Generate automated reports and dashboards for management and security analysts.
- Provide early warnings to guide resource allocation, patch management, and incident response.

V. RESULTS AND DISCUSSION

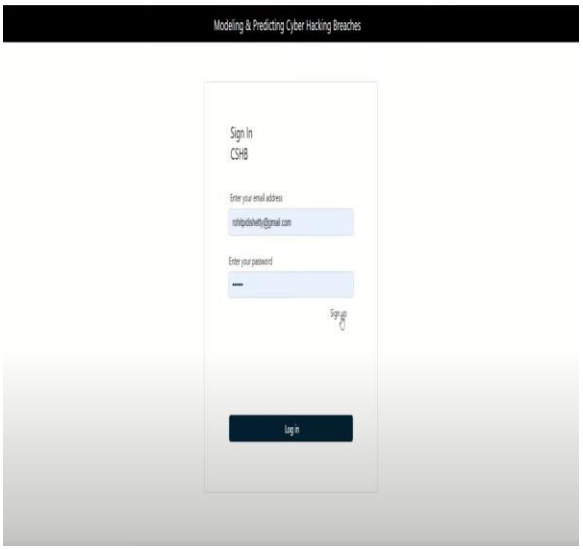

Fig 1

The diagram shows the login interface titled "Sign In" to CMA. The user is prompted to "Enter your email address" and "Enter your password" in the respective input fields. A sample email address (sample@gmail.com) is already filled in the email field, and the password field is masked. There is a button labelled "Log in" at the bottom for submitting the credentials. The layout is minimal and focused, with a professional appearance.

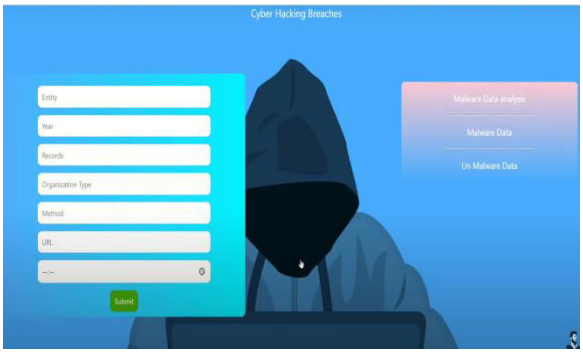

Fig 2

The image shows the digital interface or screen, predominantly featuring a vibrant blue background. In the upper portion, a light blue rectangular box contains a series of six vertical white bars or columns, suggesting data visualization or a sequential display. Below this, a large, dark, possibly black, fish-like shape is prominently centered, appearing as a silhouetted figure against the blue backdrop. Towards the bottom right, a faint, translucent rectangular shape with an orange hue is visible, adding another layer to the visual composition. The entire scene is framed within a selection box, indicating it is likely an image or object being manipulated on a screen.

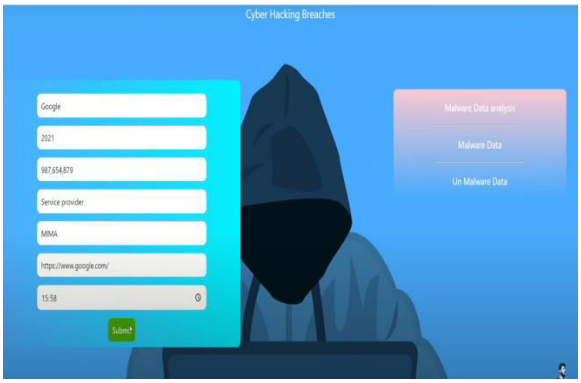

Fig 3

The image displays a user interface, likely a web page or application, with elements suggesting a login or registration form, possibly related to "Cyber Hacking" based on the text at the top.

Here's a breakdown of what's visible:

Title: "Cyber Hacking" (partially visible).

Input Fields: Several labeled input fields are present, including "Google", "JWT", "API", "Service provider", "Email", and a field with a URL "https://www.google.com".

Action Button: A green button labelled "Submit" is visible at the bottom of the form.

Additional Elements: On the right side, there are elements labelled "Malware Scan" and "Last Malware Scan".

Background Image: A silhouette of a hooded figure is visible in the background, commonly associated with hacking or cyber security themes.

Fig 4

The image shows thespread sheet or data table, likely within an application like Excel or a similar online spread sheet tool.

Key information visible includes:

Data Columns: Columns for "SN", "HOST", "TYPE", "RECORD", "TIME", "URL/Local Domain", and "ATTACK" are present.

SampleData: Entries like "Google", "Yahoo", "Public", "Private", along with numerical values and URLs like "https://www.google.com"or"https://www.greatfire.com", suggest tracking or analysis of network activity or website access.

VisualElements: A graph or chart is partially visible at the bottom, along with an illustration of a person working on a laptop, indicating data visualization and analysis are part of the displayed interface.

Context: The "ATTACK" column with "On Malware" entries suggests a security or threat analysis context.

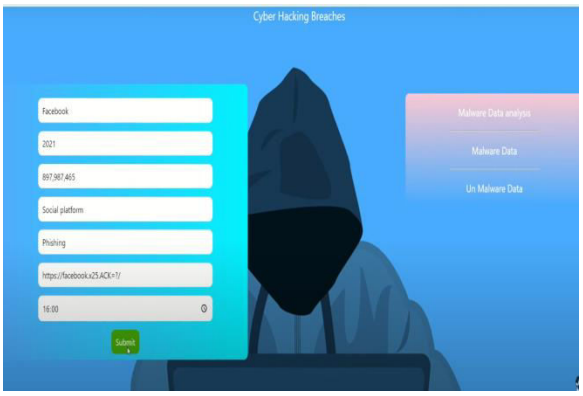

Fig 5

The image displays a screen titled "Cyber Hacking Broache," featuring a form with fields likely related to social media and a background image of a person in a hooded garment, commonly associated with hacking or anonymity. The screen is labelled "Cyber Hacking Broache." A form is visible, with fields such as "Facebook," "Social platform," and "Meeting." The background shows a figure in a hooded top, often a visual representation of a hacker.

The overall context suggests a platform or tool related to cyber activities, potentially involving social media.

Fig 6

The image shows the spread sheet, likely a "Weekly Budget Sheet for Product Rollout Plan" according to search results.

The bottom of the image also shows a graphic with a person working on a laptop and a bar chart, suggesting a business or project management context for the budget sheet.

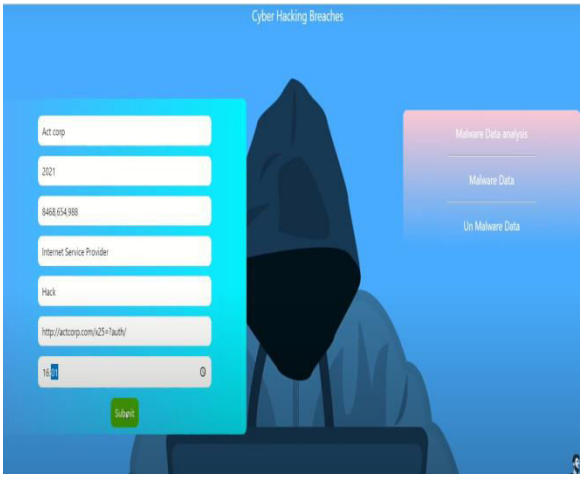

Fig 7

The image shows the several distinct text elements rather than a cohesive paragraph. The visible text includes:

Fig 8

The image contains various text elements, but a coherent paragraph is not clearly visible within the main content area. The most prominent textual content is a table and some headings.

From the visible text:

Headings: "Fig 7", "Fig 8", "AaBbCcDc", "AaBbC", "AaB", "Normal", "No Spaci...", "Heading 1", "Headi"

Table Title: "Malware - Sale Data"

Table Content (partial):

Columns with what appear to be data entries like "BAB", "F", "560560", "150048", "15", "C4BC3453", "SAB23BC", "B29A129,800 12", "60-50850045"

Other visible characters: "I", "i", "t", "t", "e", "la", "P."

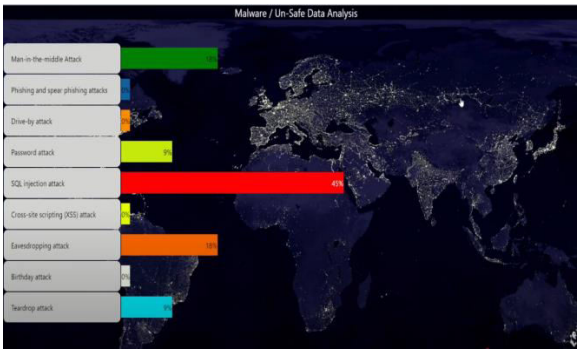

Fig 9

The image presents an overview titled "Malware / Unsafe Data Analysis," which categorizes various types of cyber-attacks. These attacks include "Man-in-the-middle Attack," "Phishing and spear phishing attack," "Drive-by attack," "Password attack," "SQL injection attack," "Cross-site scripting (XSS) attack," "Eavesdropping attack," "Botnet attack," and "Trojan attack." The visual representation also includes a bar chart indicating the prevalence or impact of these attacks, overlaid on a world map, suggesting a global perspective on these cyber security threats.

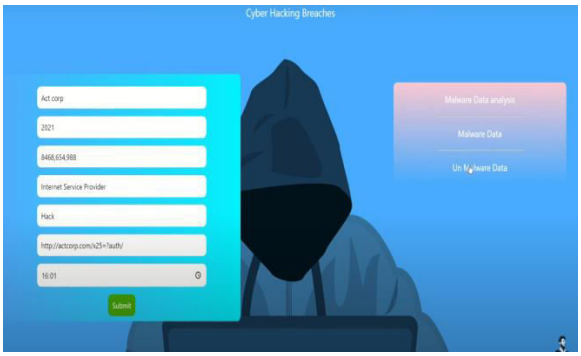

Fig 10

The image shows the partial view of a computer screen, likely running a word processing application like Microsoft Word, indicated by the "Styles" menu visible at the top. The main focus of the screen is a blue-themed interface, possibly a form or data entry screen, containing several input fields labelled with text like "AD code," "2021," "MOBILE NO," and "Internet Service Provider." A "Submit" button is also visible at the bottom of this interface. The image is labelled "Fig 10" at the bottom center.

Fig 11

The image displays a spread sheet-like interface with columns for various data points, likely related to website or network activity.

Key information visible includes:

Data Entries: Rows contain entries for "Google" and "Yahoo," with associated details like "Method," "Src Type," "Recv," "Time," and "United Resource Locator."

Website Examples: The "United Resource Locator" column shows URLs such as "https://www.google.com"and"https://www.greatsite.com."

Attack Information: The "Attack" column indicates "On Malware" for the listed entries, suggesting a security-related context.

Visual Representation: Below the table, there are graphical elements, including a person working on a laptop and a bar chart, indicating data visualization.

VI. FUTURE SCOPE AND CONCLUSION

We examined a dataset of hacker breaches concerning the inter-arrival time of incidents and the magnitude of the breaches, demonstrating that both should be described using stochastic processes instead of distributions. The statistical models presented in this research demonstrate adequate fitting and predictive accuracy. We suggest employing a copula-based methodology to forecast the combined chance of an incident occurring with a specific magnitude of breach size within a forthcoming time frame. Statistical analyses indicate that the approaches described in this study surpass those documented in the literature, as the latter neglects both temporal correlations and the interdependence of event inter-arrival periods and breach magnitudes. We performed qualitative and quantitative studies to obtain additional insights. We gathered a collection of cyber security insights, indicating that the frequency of cyber hacking breach occurrences is indeed increasing; however the severity of their damage remains unchanged. The methods outlined in this research can be utilized or modified to examine datasets of a comparable sort.

REFERENCES

1. S. Subroto and D. Apriyana, "Cyber Risk Prediction Using CVE Summary and Twitter Chatter with ANN and Machine Learning Classifiers," in Proceedings of the International Conference on Cyber security and Cyber Resilience, pp. 23-28, 2019.
2. S. Sarkar, M. S. Islam, N. H. Kim, and R. K. Chouhan, "Predicting Cyber Attacks Using Dark Web and Social-Sensor Signals," *in* Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), *Los Angeles, CA,* USA, 2019, pp. 4943-4952.
3. X. Yuan, C. Zhang, and X. Chen, "Deep Learning Approach for Predicting Cyber-Attack Rates Using LSTM Networks," *IEEE Access*, vol. 7, pp. 160481-160490, 2019.
4. N. Srinija, S. Han, M. Allodi, and L. Massacci, "Modeling Cyber

BreachEvents Using Stochastic Processes," in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), *Genoa, Italy, 2020,* pp. 93-102.

5. R. Sharma, P. Sharma, and V. Saini, "A Hybrid Machine Learning Approach for Real-Time Cyber-Attack Prediction," International Journal of Emerging Technologies, vol. 11, no. 3, pp. 145-150, 2020.

AUTHORS PROFILE

Mr.B.AMARNATH REDDY is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his M.Tech from Vellore Institute of Technology (VIT), Vellore. His research interests include MachineLearning, programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Ms.T.PAVANI is an MCA Scholar, Dept. of MCA, In QIS College of Engineering & Technology, Ongole. His areas of interest are Machine Learning, Deep Learning.