SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

Department of Software and Systems Engineering

M.S – Main Project (2017-2018)– Abstract Evaluation

Register Number	13MSE0029
Student Name	HARISH KUMAR S
Project Domain (Capstone Project)	BIG DATA
Project Title (Capstone Project)	AN SYSTEMATIC APPROACH FOR ANALYZING CYBERCRIME OCCURENCES USING BIGDATA
Abstract	The advancements in personal computer systems and networks have created a replacement setting for criminal acts, widely referred to as cybercrime. Cybercrime incidents occurrences of explicit criminal offences that cause a heavy threat to the world economy, safety, and well-being of society. It is important to reviews and identifies the features of cybercrime incidents, their respective elements and proposes a combinatorial incident description schema. The schema provides the opportunity to systematically combine various elements or cybercrime characteristics. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that match with the offence type and subsequently with a particular incident. This matching will enable better monitoring, handling and moderate cybercrime incident occurrences. Existing System: Gordon and Ford proposed a typology consisted of two categories. • Type I offences characterize singular or discrete events facilitated by the introduction of malware programs such as keystroke loggers, viruses, and rootkits. • Type II offences are facilitated by programs that are not classified as crime ware, and they are generally repeated contacts or events from the perspective of the user.

	Cons of Existing System: The cons of an existing system are: 1) Lack of a concise classification and monitoring of the particular offences it entails. 2) The multiple interpretations of what cybercrime entails along with nonsystematic classification of the corresponding offences and lack of recommended actions are not contributing toward managing and orchestrating effective directives, policies, and legislative initiatives at local, national, or international level and result in ineffective handling of cybercrime incidents. 3) The system can process limited data and also take too much time for process data Proposed System: The proposed system was a schema-based cybercrime incident description that: 1) Identifies the features of a cybercrime incident and their potential elements 2) Provides a two-level offence classification system based on specific criteria. 3) Proposed concept deals with providing database by using Hadoop with Spark we can analyze unlimited data's and simply add number of machines to the cluster so the results are produced in less time. 4) The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that counteract the offence type and subsequently the particular incident. Advantages of Proposed System: The advantages are: 1) This system will act as a guide where the high frequency of cybercrime occurrences 2) By identifying the elements of each feature we can examine any interrelations between specific elements that would highlight specific aspects of cybercrime offences. 3) Involves the detection of the exact threat that caused the offence.
Guide Name	Prof.Kavitha B R
Guide Signature	