[1] Neelima Kant
[2] Amrita

Design and Development of Effective Cyber Threat Intelligence Platform to Improve Cyber Resilience

Abstract: - Cyber-Physical Systems (CPS) are a ubiquitous notion in which items that are networked and equipped with internet connectivity may sense and send data via a network. Examine how CPS devices might be used in a smart home setting. The Internet of Things, or IoT, has become increasingly popular because of all of its advantages, which include increased human comfort, cost effectiveness, time efficiency, and wise use of electricity. The low-capacity sensor node, which consists of many parts linked by a wireless network and can function as either hosts or clients on the internet, is the central component of the cyber-physical system. Resources such as limited processing power, storage capacity, and energy backup make traditional desktop security techniques ineffective in these systems. Introducing Secure Auth Key, a lightweight key agreement and authentication system ready to tackle confidentiality problems and security risks present in modern constraint-based CPS systems.

The intended result consists of a security algorithm that guarantees trust, security, and user data privacy without sacrificing the adaptability and autonomy of CPS devices, as well as a lightweight authentication system for cyber-physical devices. Dynamicity and scalability are ensured by an inventive middleware module that is implemented on the Raspberry platform and makes CPS-based devices and services interoperable. The main objective is to provide a flexible framework for a safe Internet of Things infrastructure and assess its efficacy in various contexts that are focused on the user.

The goal of the suggested technique is to achieve mutual authentication across CPS devices as efficiently and as little as possible in terms of computing overhead. In order to safeguard wireless connections and strengthen the system against several cyberthreats, it produces dynamic session keys. A novel lightweight security solution that balances security, performance, and cost is desperately needed, as constraint-based CPS systems have limited resources. Secure Auth Key is tested on the Smart Home System, where a proof-of-concept prototype shows the robustness of the system.

Even with modest computing power, little storage, and little energy backup, the algorithm performs well. Experiments conducted in real life, such as replay assaults, man-in-the-middle attacks, and penetration testing, highlight how effective the system is in a variety of situations. By generating fresh session keys, each 128 bits in length, the proposed technique ensures a lightweight end-to-end key formation mechanism for every session, easing worries about session expiration. This small key size helps algorithms run more quickly, and pre-configuring every device improves system security by preventing hackers from knowing the exact configuration settings.

Keywords: Artificial Intelligence, Machine Learning, Cyber Attacks, Security feeds, Cyber Resilience.

1. INTRODUCTION

The threat of cyberattacks is becoming more and more real in the modern digital age, as the web of global commerce and society is becoming more and more interwoven with the digital world. Cyberattacks have become a constant and ubiquitous threat to both individuals and companies, ranging from opportunistic cybercriminal actions to sophisticated nation-state efforts [1]. The imperative requirement for an efficient Cyber Threat Intelligence (CTI) platform to strengthen cyber resilience is highlighted by the swift development of these threats and their capacity to inflict severe disruptions and monetary losses. Cyber resilience is the ability of an organization to minimize the effects of cyberattacks while simultaneously adapting, recovering, and carrying on with its operations [2]. As cyber enemies constantly innovate and modify their tactics, strategies, and procedures, achieving cyber resilience is a never-ending problem. Organizations need to take a proactive, intelligence-driven approach in order to successfully traverse this constantly shifting terrain [3]. This strategy's mainstay is an extensive CTI platform made to gather, examine, and distribute useful threat intelligence. As the digital sentinel, this platform keeps a close eye on the digital landscape for any indications of potential risks, weaknesses, or malicious activity. Its importance is immense because it enables enterprises to shift from reactive cybersecurity measures to proactive threat mitigation.

A rich tapestry of technology, knowledge, and cooperative efforts are included into the design and development of an efficient CTI platform, which are complex undertakings. An extensive range of data sources, including internal network logs, threat intelligence feeds, open-source feeds, and more, must be smoothly ingested by such a platform [4]. Modern technologies such as artificial intelligence and machine learning are needed to process this

[1]Computer Science & Engineering, Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh - 201306, India
[2] Centre for Cyber Security and Cryptology, Computer Science & Engineering, Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh - 201306, India

flood of data, find patterns, and extract useful information [5]. A well-designed CTI platform emphasizes cooperation and information sharing, which is one of its defining characteristics. Nobody has a full picture of the threat landscape while dealing with opponents who are always evolving [6]. Therefore, companies need to adopt a collective defensive strategy, exchanging intelligence with government agencies and other industry sectors in addition to within their own ranks. [7].

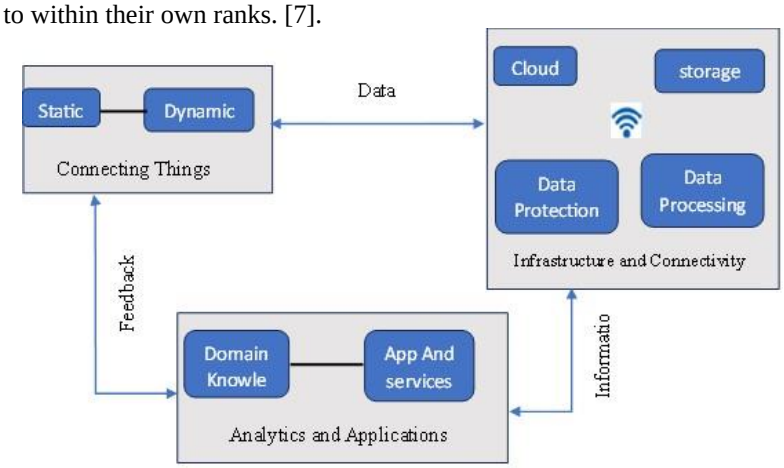

Figure 1: Cyber Physical System Components

Figure 1 shows the CPS's constituent parts. These elements specified how CPS was implemented in various applications. There are three main components to the CPS architecture. Items or Relatives Processing and infrastructure Additionally, this CTI platform is a strategic asset that uses automation and analytics to supplement human expertise, not just a technology stack [8]. It enables cybersecurity teams to respond quickly and intelligently by optimizing algorithms, reducing false positives, and guaranteeing the timely delivery of high-confidence warnings. In this era where the digital landscape continuously evolves, the CTI platform stands as a beacon of hope in the battle against cyber threats. Its development represents an imperative step in enhancing an organization's cyber resilience [9].

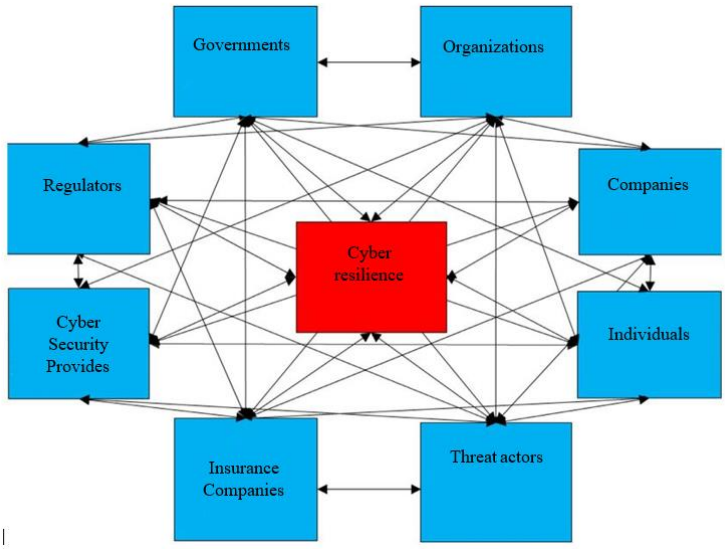

Figure 2: Representatives of the Cyber Resilience Actors.

They might abide by customs, regulations, guidelines, and protocols. A few of the actors and their roles in cyber resilience in an effort to highlight important players that are important for both maintaining and jeopardising cyber resilience. Any type of link or contact is specified by the two-way arrows in Figure 2 [10]. Though in certain circumstances one-way arrows may be applicable, we often presume two-way arrows. Cyber resilience affects some actors more than it affects them, and vice versa for other actors. The eight types of actors each have a distinct role that relates to cyber resilience in many ways. For instance, governments favour increased cyber resilience within their borders since it benefits a large number of businesses, organisations, and people [11]. Threat actors, on the other hand, who might be either singular entities or groups, would rather weaken cyber resilience or take advantage of weak cyber resilience. In order to have something to offer, cyber security companies could want to

have technology that is readily available but lacks cyber resilience [12]. A situation that permits regulation and insurance to have an impact on cyber resilience may be preferred by regulators and insurance providers.

1.1. Cyber resilience in the future

The current status of the internet of things, or IoT, is immature. With the exception of being specifically designed for autonomous interaction and communication between objects, the Internet of Things is similar to the standard internet. Nowadays, most of our interactions are manual and very few things that we utilise are online. For instance, we speak with an oven when we use the internet to switch on the heat in the cabin [13]. Many items created by humans may eventually be accessible online with increasingly automated and sophisticated communication. For instance, when the GPS tracker determines where the car is going, our vehicle might activate the inside heating. IoT includes smart equipment that can do things like turn on the heat in the cabin. Such gadgets, especially when used in large quantities, can have a significant impact on the physical infrastructure, such as metro operations or the transmission and distribution components of the electricity grid, which are not IoT in and of themselves [14]. Undoubtedly, the Internet of Things will make many of our daily jobs easier, but it will also make things easier for terrorists, for example. It will become unnecessary to physically take control of a truck or aeroplane, and it might even become less essential to commit suicide by blowing oneself up [15]. IoT continues to expand its electronic reach, potentially leading to a catastrophic incident in large cities, such as the metro. In general, technical and organisational reasons, the IoT, numerous standards, and the flexible nature of organisations will all have an increased impact on cyber resilience in the future.

2. Background and literature survey

2.1. Review of completed work and the need for additional study

Cyberattacks against CPS are prevented by a multitude of security mechanisms and procedures. The standard method repels attackers by utilizing the security systems already in place. However, these days, attackers can easily get beyond the limitations of more traditional techniques. Wearing airtights A few of the software tools used in CPS networks to initiate attacks and steal data are WIPS, Aerohived, ethereal, and others. Academic and industry researchers are working together to develop stronger defenses against cyberattacks on CPS. Numerous scholars are concentrating on the subject of cyber-physical system security [16]. They have proposed several tactics to stop CPS attacks. Precautions against an attack were also suggested. A secure communication protocol is being developed by multiple researchers to increase communication security. Different solutions take different assumptions into account [17]. Certain solutions adopt a proactive approach, whereas others adopt a reactive one. IT attacks are used to provide a review of the literature on CPS. Several publications recommend different security strategies. Some articles are surveys that list security-related problems, challenges, and fixes. A security framework is also suggested by a number of studies. To safeguard the CPS system, a number of researchers are working on a machine learning technique.

In the ever-evolving landscape of cybersecurity threats, the development and deployment of a robust Cyber Threat Intelligence (CTI) platform is now critical to enhancing organizational cyber resilience. The foundation of this project is based on the increasing complexity and diversity of cyber attacks that pose a major risk to critical infrastructure and sensitive data [18]. Devoted to building a robust CTI platform, a team of software engineers and cybersecurity experts recognized that a proactive and adaptable approach was necessary. By gathering, evaluating, and disseminating relevant and up-to-date threat intelligence, this platform aims to help organizations better identify, counter, and mitigate cyber threats. The platform uses machine learning, threat intelligence feeds, and advanced analytics to provide users with a comprehensive and current picture of the threat landscape [19]. The goal of this CTI platform's design and development is to fortify organizational defenses by encouraging cooperation and information exchange among cybersecurity experts. In the end, this will help create a digital environment that is more secure and robust.

2.2. CPS security survey: obstacles and approaches

In their taxonomy assessment of the security situation, Mario Frustaci et al. examine the three primary core levels of the Internet of Things system model: perception, transportation, and application level. The analysis's conclusions highlight the main problems and provide direction for more study. It also draws a contrast between IoT security and conventional IT security. The topic of physical access security was also brought up. The author also provided solutions for a number of IoT device risks [20]. Lastly, the author makes the case that because of the physical exposure of IoT devices, their lack of resources, and their varied technological makeup, the Perception Layer is the most susceptible level of the IoT system architecture. This implies that constrained cyber-physical devices have restrictions, which is why it's crucial.

Information about problems, difficulties, and solutions pertaining to smart home security systems is presented by Komninos, N. et al. The authors classed different assaults according to their impact and security objectives. The author focuses on issues related to smart home security, which are elements of the smart grid. In certain instances, they seem to constitute a risk to the ecology of smart homes and smart grids [21]. The vulnerabilities found are categorised based on the specific security objectives of the smart home/smart grid environment, and their impact on the overall network security is evaluated. (Pitsillides, Philippou, and Kaminos, 2014).

These networks will be secured by the TLS (Transport Layer Security) and DTLS (Datagram Transport Level Security) protocols, which will connect the internet to low-power and lossy networks. End-to-end security is essential for securing Internet of Things devices [22]. Due of a variety of possible use cases, such as CoAP, DTLS, and HTTP/CoAP, each with individual requirements and constraints, TLS/DTLS was interrupted by a 6LBR. The author discussed three security issues and two countermeasures that lead to resource depletion in the Low-power and Lossy Network (LLN). To guarantee end-to-end security at the application layer and stop the 6LBR from accessing data while it is in transit, they use the first approach, which maps TLS to DTLS.
provide a security study of the various CPS security methodologies, risk assessment, and design layers. Ultimately, the difficulties, directions for further study, and possible fixes are examined and outlined. Since there is a lot of confusion between CPS and IoT, the terms have been used interchangeably. The article claims that although academic institutions favour CPS, companies and government agencies favour IoT. The author also discussed some attacks that were directed on CPS. The author also addressed the risk assessment for each attack [24]. According to the paper's author, Identity-Based cryptography is a common cryptographic encryption methodology that uses short encryption keys and is thought to execute and compute more effectively than other cryptosystem techniques.

2.3. Problem statement

In the digital age, organisations face a significant challenge from the increasing complexity and diversity of cyber threats. The absence of a comprehensive and adaptable Cyber Threat Intelligence (CTI) platform impedes the proactive detection, mitigation, and response to dynamic threats, even with the progress made in cybersecurity measures. Current systems frequently have difficulty using advanced analytics, integrating many data sources, and promoting productive stakeholder collaboration in cybersecurity. Organisations are exposed to sophisticated cyberattacks that take use of newly discovered vulnerabilities when there is a lack of a unified CTI platform, which worsens the risk environment [25]. A purpose-built CTI platform that not only gathers and analyses threat intelligence in real-time but also promotes an ecosystem of collaboration for information sharing throughout organisations is desperately needed in light of these difficulties. By tackling this issue, organisations in a variety of sectors will be far more cyber resilient, protecting vital infrastructure and sensitive data while also guaranteeing a proactive defence against the constantly shifting cyber threat scenario.

2.4. Research gap

- Research in automation and orchestration could look into ways to improve these characteristics within cyber threat intelligence platforms in order to expedite the gathering, processing, and distribution of threat intelligence. This entails creating complex algorithms for automatic reaction and decision-making.
- Examine the most recent developments in machine learning and artificial intelligence to increase the accuracy and effectiveness of threat identification and classification [26]. This could entail developing models that can identify novel and cutting-edge cyberthreats.
- It is essential to integrate human-centric methodologies into cyber threat intelligence, acknowledging the significance of human proficiency in evaluating intricate threats and arriving at well-informed conclusions. This field of study may include the creation of intuitive user interfaces and potent visualisation techniques.
- Research should concentrate on techniques for managing and sharing threat intelligence while respecting people's right to privacy, given the growing emphasis on privacy. This includes investigating the moral ramifications of particular intelligence methods.
- Research should focus on creating methods and tools to improve the security of digital supply chains due to the increasing complexity of supply chain threats [27]. This covers techniques to confirm the integrity and security of both software and hardware components.
- For the most up-to-date information about research gaps in cyber threat intelligence, it is essential to keep up with latest publications, conferences, and journals, as the field may have changed since my last update.

3. Proposed Methodology

The cyber-Physical system is made up of several wirelessly networked low-capacity devices (sensors, micro-controllers, and other devices). Smart devices on the network need to talk to one other and do their business securely. Unfortunately, there aren't many common security measures that can offer sufficient protection because of resource limitations including low processing power, limited energy, and restricted space [28]. The session key created by the algorithm is called SecureAuthKey. Secure communication between two devices in the cyber-physical system realm is the primary objective of SecureAuthKey.

3.1. SecureAuthKey

A brief explanation of the suggested algorithm with the name SecureAuthKey is given below. Another name for it is the Key Agreement Algorithm. It is used to allow mutual authentication between two connected devices in a cyber-physical system. Every time two interacting devices establish a new communication session, a dynamic session key is generated. This technique is unusual in that it creates a different dynamic session key for every communication step.

3.2. SecureAuthKey: An Algorithm for Creating Session Keys

Client codes or end points for Cyber Physical systems that are attached to microcontrollers are developed. Another name for a microcontroller is a gateway server. Every client node—also referred to as a smart device—is linked to the gateway server. For applications built on CPS, a gateway server serves as a single point of connection. Wired networks (IEEE 802.3) or wireless networks (IEEE 802.11) are used to connect client nodes to microcontrollers [29]. kilobytes to implement the SecureAuthKey Algorithm. According to Naveen Kumar and Thite (2022), Figure 3 displays the parameters used in the SecureAuthKey Key agreement Algorithm, the various keys utilised in the SecureAuthKey Algorithm. Key characteristics of cyber-physical systems (CPS) are displayed in Figure 4.

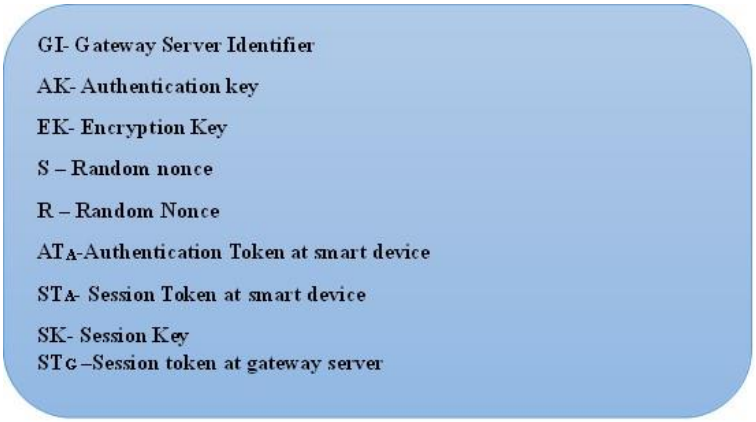

Figure 3: SecureAuthKey Key Agreement Algorithm Parameters

Figure 4: Cyber-Physical Systems' Five Essential Properties [38]

3.3. Activity diagram Activity at the Gateway server

The activity diagram at the gateway server side is displayed in Figure 5. The gateway server initialises and uses the access point to connect to the wireless network. It connects to a smart device using a socket. The communication port and IP addresses are contained in the socket. To connect to network devices that are a member of the network, a connection handler module is utilised [32]. The data handler module uses many communication keys to function. which covers session keys, encryption, and authentication [37]. The many tasks carried out by the gateway server include extracting random nonce information, creating an authentication token, and comparing it with the authentication token received by the smart device [36]. The creation of a session key and sending it to another device for authentication purposes is the final, crucial step.

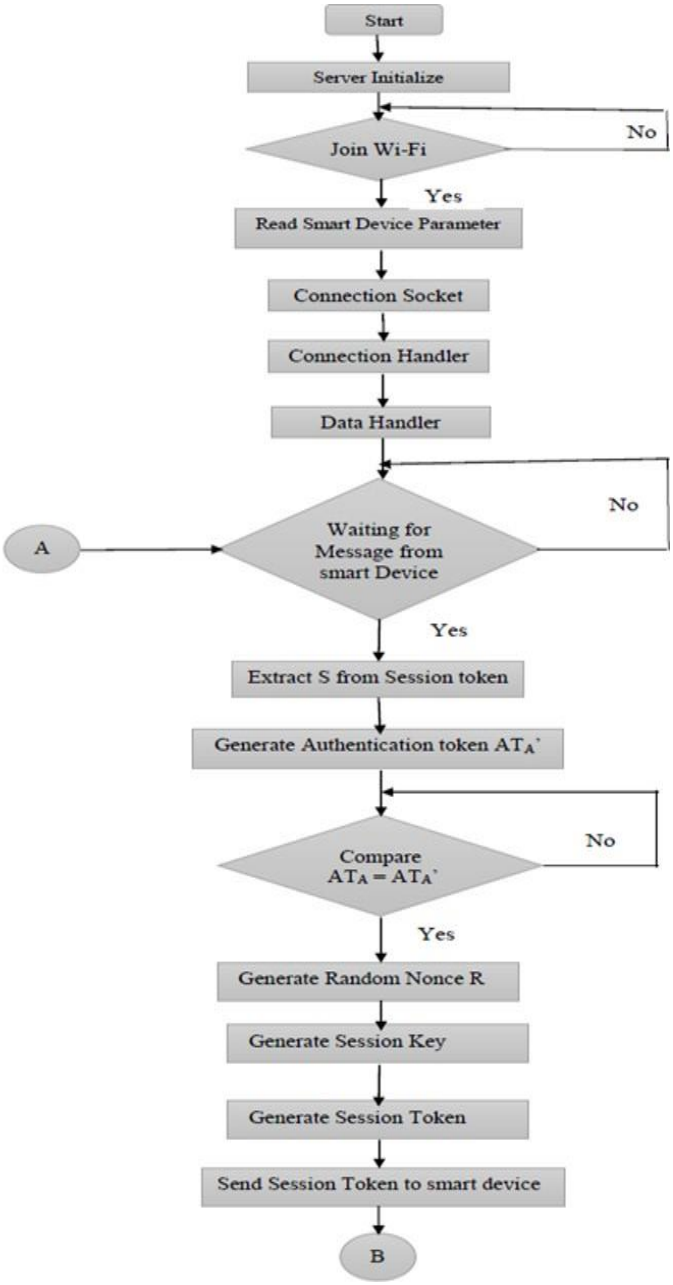

Figure 5: Activity diagram at Gateway server [32]

3.4. Class Diagram

An object collection with shared qualities is called a class. A class diagram illustrates a collection of classes and shows how they collaborate and relate to one another [33]. Figure 6's class diagram illustrates a secure CPS application that uses the Smart Device class to operate on a smart device. Class The functions and parameters needed for algorithm execution at the gateway server are defined by Gateway Server. For encryption and decryption, use Message Digest, Credential Holder, Gateway Server, and AES.

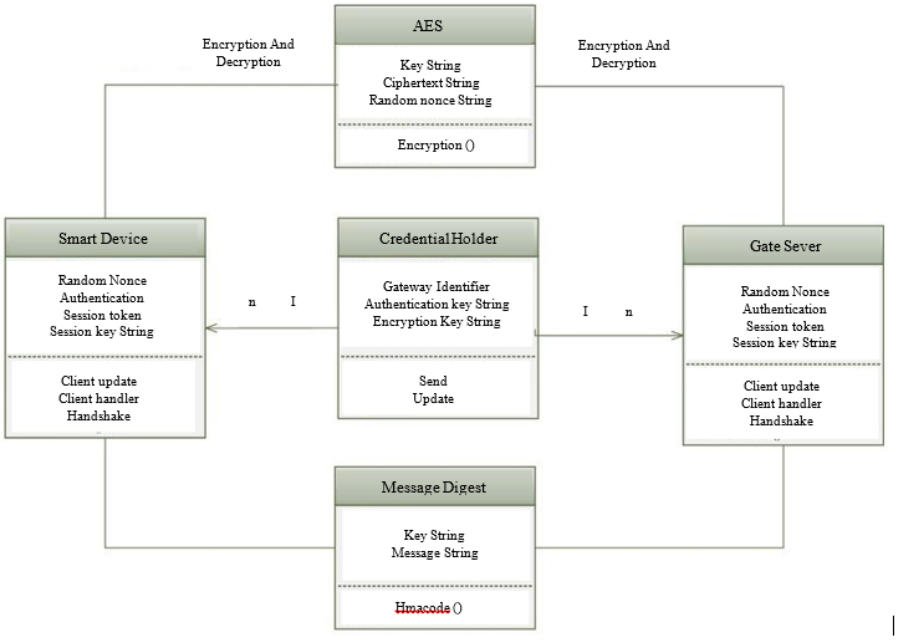

Figure 6.: Class Diagram for Secure CPS Application [35]

Classes are created from groups of objects that share similar characteristics. A class diagram shows a group of classes, their connections, and the group members' cooperative activities. Figure 6's class diagram illustrates the secure CPS application, which uses the Smart Device class to perform actions at the smart device [34]. class the functions and parameters required for the gateway server to execute algorithms are specified by the gateway server. In addition to Credential Holder, Gateway Server, and Message Digest, AES is employed for encryption and decryption.

4. RESULT DISCUSSION

The creation and implementation of a safe Cyber-Physical System (CPS) application are the main objectives of the project, which focuses on the interactions between different components such gateway servers, smart devices, and communication protocols. The objective of the experiment is to create a secure CPS application that guarantees data confidentiality, integrity, and authentication while facilitating communication and interaction between smart devices and a gateway server. The CPS application's class diagram shows the hierarchy and connections between its various classes. Smart Device, Credential Holder, Gateway Server, Message Digest, and AES (for encryption and decryption) are some of the important classes that are listed. The collaboration and interaction between these classes to carry out different tasks within the programme are shown in the diagram.

Table 1. displays the running of a programmer at various intervals. 15 distinct time intervals are taken and programmers are run.

Table 1. displays the system time, user time, and real time following each interval.

Time interval	Real time	User time	System time
1	0.069	0.061	0.008
2	0.070	0.066	0.004
3	0.067	0.066	0.004
4	0.067	0.055	0.010
5	0.065	0.049	0.016
6	0.065	0.061	0.004
7	0.064	0.053	0.012
8	0.064	0.033	0.031
9	0.063	0.059	0.004
10	0.063	0.048	0.016
11	0.064	0.056	0.008
12	0.065	0.053	0.012
13	0.066	0.055	0.012
14	0.066	0.058	0.008

15	0.065	0.058	0.008
Total	**0.984**	**0.833**	**0.158**
Average	**0.066**	**0.056**	**0.12**

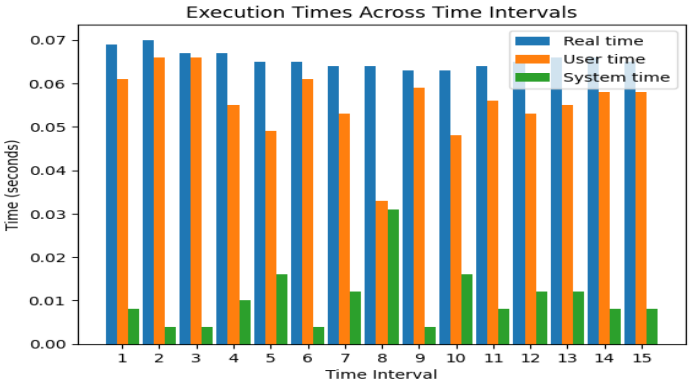

Figure 7. Display real-time, system time, and user time at regular intervals.

Table 2. Smart device operations at varying time intervals.

Time interval	**real time**	**User time**	**System time**
1	0.063	0.05	0.013
2	0.065	0.047	0.017
3	0.056	0.044	0.012
4	0.064	0.052	0.012
5	0.066	0.057	0.009
6	0.065	0.048	0.017
7	0.069	0.057	0.011
8	0.071	0.055	0.016
9	0.063	0.058	0.005
10	0.066	0.061	0.005
11	0.066	0.053	0.013
12	0.063	0.051	0.012
13	0.067	0.058	0.009
14	0.064	0.044	0.02
15	0.064	0.051	0.013
16	0.062	0.057	0.005
17	0.062	0.041	0.021
18	0.064	0.056	0.008
19	0.062	0.053	0.009
20	0.065	0.053	0.013
Total	**1.287**	**1.046**	**0.24**
Average	**0.064**	**0.052**	**0.012**

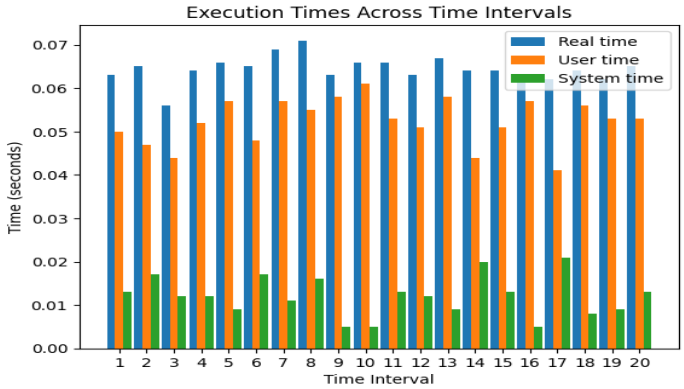

Figure 8. Smart devices run at different intervals of time.

The last two were included because they are the most well-known devices for specialised IoT applications with active communities, and their data will assist our model better incorporate the technical IoT language. The used data dumps contain user interactions shown as Q&As along with content from posts, comments, and related tags in XML format. To enhance the dataset and subsequently the vocabulary, the XML data files are downloaded and processed on a regular basis.

Table 3. Performance comparison of best Classifiers

Metric	Classifier	Train CVE-Test CVE	Train CVE-Test No CVE	Train No CVE-Test CVE	Train No CVE-Test No CVE
Accuracy	Random Forest	0.8373	0.8361	0.8571	0.8571
	CNN	0.8452	0.8153	0.8462	0.8384
Precision	Random Forest	0.8149	0.8326	0.8952	0.8295
	CNN	0.8149	0.8716	0.8174	0.8959
Recall	Random Forest	0.8571	0.8201	0.8305	0.8305
	CNN	0.8351	0.8524	0.8862	0.8921
F1_score	Random Forest	0.8245	0.8642	0.8907	0.8907
	CNN	0.8941	0.8937	0.8434	0.8143

an analysis of how well your system performs in an environment that is representative of the actual world by means of a monitoring cycle that makes use of the Twitter Stream API and a categorization procedure. This examination was carried out not once but twice, and each time a unique collection of input phrases was utilized.

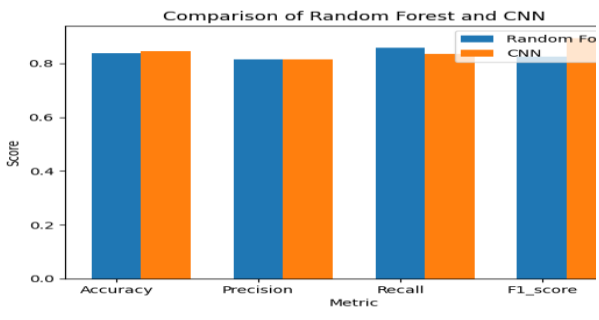

Figure 9. A comparison of the top classifiers' performances

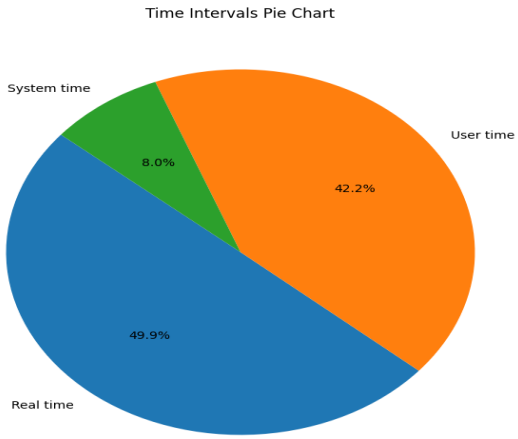

Figure 10. temporal interval pie chart Programme execution

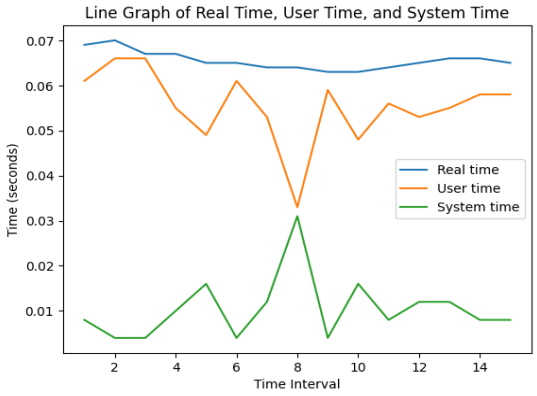

Figure 11. real-time execution line graph

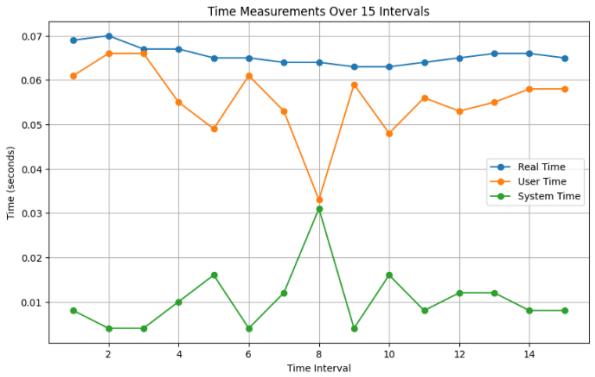

Figure 12. Programme execution on smart devices

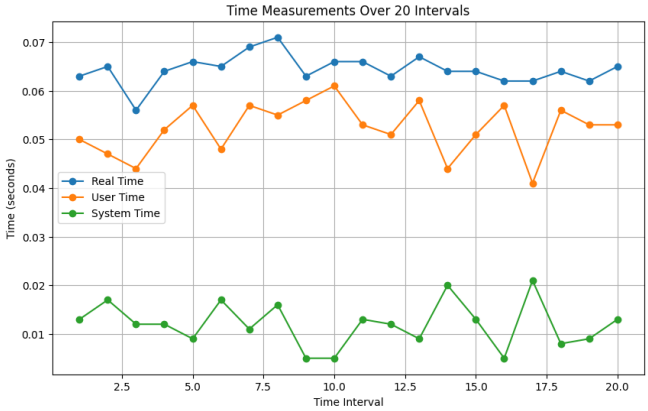

Figure 13. Microcontroller programme execution duration

5. Future Research

Future studies should examine cyber resilience in greater detail, going beyond the scope of this article by focusing on at least seven key areas. In order to account for the evolving cyber landscape, there should first be a systemic and technical focus on controls, measures, and recovery procedures. Secondly, an emphasis on qualities of the organisation such as relationships of trust, autonomy, and procedures for recovery. The third is an emphasis on human behavioural patterns, such as habits, security awareness, and attitudes. The fourth is an emphasis on rules and regulations. The fifth is an emphasis on growing into the future, adjusting to the present, and learning from the past. Sixth, gathering past information on cyber incidents and the reasons for systemic, human, organisational, and strategic mistakes as well as their outcomes. Seventh, given that grey swans are thought to be frequent in cyberspace, it is possible that actors that are cyber-resilient will be better equipped to handle them. Grey swans are identified from black swans , which are known unknowns, and white swans, which may be verified empirically. Future studies ought to evaluate if actors who are cyber-resilient would be better equipped to handle unknown unknowns.

6. Conclusion

The paper examines and evaluates the growing significance of cyber resilience. First, a wide range of entities that can be categorized as threat, hybrid, and non-threat actors are involved in cyber resilience. Governments, regulators, and other non-threat players can insurers, individuals, organizations, and incident responders. Hackers and criminals are examples of threat actors. Companies that occasionally, whether on purpose or accidentally, jeopardize other actors' cyber resilience are considered hybrid actors. Actors function on multiple levels: the person, the group, the organization, the region, etc., and the global level. Cyber resilience influences and is influenced by the values and inclinations of each actor while choosing tactics. Second, modern definitions of cyber resilience define it as the ability of an actor to continue operating as usual despite, responding to, and recovering from cyber incidents. Third, the players are identified who are impacted by and affected by cyber resilience. Everybody else's cyber resilience and strategy is impacted by the array of tools, resources, knowledge, and technology that these actors possess. Fourth, there is a connection between cyber resilience and cyber insurance through a number of services such as incident response, data gathering from claims, cover limitations depending on current security measures, and preconditions or entrance requirements for cyber contracts that influence pricing. Fifth, a role for cyber resilience that is focused on the future is described. Cyber resilience is linked to the internet of things, and it is expected that this technology will improve many aspects of life, including artificial

intelligence and machine learning. A wide attack surface, insufficient technology, challenging data processing, possible over-reliance on computers and software, and ethical concerns are just a few of the obstacles facing the internet of things. Cyber resilience is also associated with the use of robots by firemen in the event of a data centre fire, for example. Finally, a number of recommendations for further study are made.

REFERENCE

[1] Ahmadi-Hamadi-Assalemi, G. et al. (2020). "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review." Smart Cities, 3(3), 894–927. DOI: 10.3390/smartcities3030046.

[2] Bhushan, K., & Gupta, B.B. (2019). "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment." Journal of Ambient Intelligence and Humanized Computing, 10, 1985–1997.

[3] Najork, M. (2009). "Web Crawler Architecture." In Encyclopedia of Database Systems. Springer: New York, NY, USA, 3462–3465.

[4] Quoc, D.L., Fetzer, C., Felber, P., Rivière, E., Schiavoni, V., & Sutra, P. (2015). "UniCrawl: A Practical Geographically Distributed Web Crawler." In Proceedings of the 8th IEEE International Conference on Cloud Computing (Cloud 2015), 389–396.

[5] Vikas, O., Chiluka, N.J., Ray, P.K., Meena, G., Meshram, A.K., Gupta, A., & Sisodia, A. (2007). "WebMiner—Anatomy of Super Peer Based Incremental Topic-Specific Web Crawler." In Proceedings of the Sixth International Conference on Networking (ICN 2007), 32.

[6] Gupta, K., Mittal, V., Bishnoi, B., Maheshwari, S., & Patel, D. (2016). "ACT: Accuracy-Aware Crawling Techniques for Cloud-Crawler." World Wide Web, 19, 69–88.

[7] Li, Y., Zhao, L., Liu, X., & Zhang, P. (2014). "A Security Framework for Cloud-Based Web Crawling System." In Proceedings of the 11th Web Information System and Application Conference (WISA 2014), 101–104.

[8] Gaur, R., & Sharma, D.K. (2014). "Focused Crawling with Ontology Using Semi-Automatic Tagging for Relevancy." In Proceedings of the Seventh International Conference on Contemporary Computing (IC3 2014), 501–506.

[9] Pham, K., Santos, A.S.R., & Freire, J. (2018). "Learning to Discover Domain-Specific Web Content." In Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining (WSDM 2018), 432–440.

[10] Singh, M.P. (2004). "The Practical Handbook of Internet Computing." CRC Press, Inc.: Boca Raton, FL, USA.

[11] Jiang, J., Yu, N., & Lin, C. (2012). "Focus: Learning to Crawl Web Forums." In Proceedings of the 21st World Wide Web Conference (WWW 2012), Companion Volume, 33–42.

[12] Sachan, A., Lim, W., & Thing, V.L.L. (2012). "A Generalized Links and Text Properties-Based Forum Crawler." In Proceedings of the 2012 IEEE/WIC/ACM International Conferences on Web Intelligence (WI 2012), 113–120.

[13] Yang, J., Cai, R., Wang, C., Huang, H., Zhang, L., & Ma, W. (2009). "Incorporating Site-Level Knowledge for Incremental Crawling of Web Forums: A List-Wise Strategy." In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1375–1384.

[14] Wang, Y., Yang, J., Lai, W., Cai, R., Zhang, L., & Ma, W. (2008). "Exploring Traversal Strategy for Web Forum Crawling." In Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 2008), 459–466.

[15] Cai, R., Yang, J., Lai, W., Wang, Y., & Zhang, L. (2008). "iRobot: An Intelligent Crawler for Web Forums." In Proceedings of the 17th International Conference on World Wide Web (WWW 2008), 447–456.

[16] Guo, Y., Li, K., Zhang, K., & Zhang, G. (2006). "Board Forum Crawling: A Web Crawling Method for Web Forum." In Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2006), 745–748.

[17] Hurst, M., & Maykov, A. (2009). "Social Streams Blog Crawler." In Proceedings of the 25th International Conference on Data Engineering (ICDE 2009), 1615–1618.

[18] Agarwal, S., & Sureka, A. (2015). "A Topical Crawler for Uncovering Hidden Communities of Extremist Micro-Bloggers on Tumblr." In Proceedings of the 5th Workshop on Making Sense of Microposts co-located with the 24th International World Wide Web Conference (WWW 2015), 26–27.

[19] Chau, D.H., Pandit, S., Wang, S., & Faloutsos, C. (2007). "Parallel Crawling for Online Social Networks." In Proceedings of the 16th International Conference on World Wide Web (WWW 2007), 1283–1284.

[20] Zhang, Z., & Nasraoui, O. (2008). "Profile-Based Focused Crawler for Social Media-Sharing Websites." In Proceedings of the 20th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2008), Volume 1, 317–324.

[21] Buccafurri, F., Lax, G., Nocera, A., & Ursino, D. (2012). "Crawling Social Internetworking Systems." In Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012), 506–510.

[22] Khan, A., & Sharma, D.K. (2017). "Self-Adaptive Ontology Based Focused Crawler for Social Bookmarking Sites." IJIRR, 7, 51–67.

[23] Ferreira, R., Lima, R., Melo, J., Costa, E., de Freitas, F.L.G., & Luna, H.P.L. (2012). "Retriblog: A Framework for Creating Blog Crawlers." In Proceedings of the ACM Symposium on Applied Computing (SAC 2012), 696–701.

[24] Valkanas, G., Ntoulas, A., & Gunopulos, D. (2011). "Rank-Aware Crawling of Hidden Web Sites." In Proceedings of the 14th International Workshop on the Web and Databases 2011 (WebDB 2011).

[25] Wang, Y., Lu, J., Chen, J., & Li, Y. (2017). "Crawling Ranked Deep Web Data Sources." World Wide Web, 20, 89–110.

[26] Zhao, F., Zhou, J., Nie, C., Huang, H., & Jin, H. (2016). "SmartCrawler: A Two-Stage Crawler for Efficiently Harvesting Deep-Web Interfaces." IEEE Trans. Serv. Comput., 9, 608–620.

[27] Zheng, Q., Wu, Z., Cheng, X., Jiang, L., & Liu, J. (2013). "Learning to Crawl Deep Web." Inf. Syst., 38, 801–819.

[28] Jiang, L., Wu, Z., Feng, Q., Liu, J., & Zheng, Q. (2010). "Efficient Deep Web Crawling Using Reinforcement Learning." In Proceedings of the Advances in Knowledge Discovery and Data Mining, 14th Pacific-Asia Conference (PAKDD 2010), Part I, 428–439.

[29] Madhavan, J., Ko, D., Kot, L., Ganapathy, V., Rasmussen, A., & Halevy, A.Y. (2008). "Google's Deep Web Crawl." PVLDB, 1, 1241–1252.
[30] Rösch, D., Bauer, T., Kummerow, A., Kühne, M., Nicolai, S., & Bretschneider, P. (2023). "Transformation in Substation Automation: Cyber-Resilient Digital Substations (CyReDS) in Power Grids." AT-Automatisierungstechnik, 71(9), 789-801.
[31] McLaughlin, K. (2023). "Cybersecurity Deception Engineers: The Unseen Guardians of Cybersecurity Programs and the Unsung Heroes in the Battle Against Cyber Threats." EDPACS, 1-6.
[32] Weisman, M.J., Kott, A., Ellis, J.E., Murphy, B.J., Parker, T.W., Smith, S., & Vandekerckhove, J. (2023). "Quantitative Measurement of Cyber Resilience: Modeling and Experimentation." arXiv preprint arXiv:2303.16307.
[33] Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). "The Tensions of Cyber-Resilience: From Sensemaking to Practice." Computers & Security, 132, 103372.
[34] Salvi, A., Spagnoletti, P., & Noori, N.S. (2022). "Cyber-Resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem." Computers & Security, 112, 102507.
[35] Ammi, M., Adedugbe, O., Alharby, F.M., & Benkhelifa, E. (2022). "Leveraging a Cloud-Native Architecture to Enable Semantic Interconnectedness of Data for Cyber Threat Intelligence." Cluster Computing, 25(5), 3629-3640.
[36] Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., & Linkov, I. (2022). "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks." IEEE Transactions on Intelligent Transportation Systems, 24(1), 1000-1014.
[37] Ligo, A.K., Kott, A., & Linkov, I. (2021). "How to Measure Cyber-Resilience of a System with Autonomous Agents: Approaches and Challenges." IEEE Engineering Management Review, 49(2), 89-97.
[38] Kott, A., & Linkov, I. (2021). "To Improve Cyber Resilience, Measure It." arXiv preprint arXiv:2102.09455.
[39] Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. (2020). "TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data." Computers & Security, 95, 101867.