IOT BASED CLOUD COMPUTING APPLICATION AND THEIR SECURITY

Dr. Ravindra S. Apare1, Dr. Manoj L. Bangare2, Dr. Pushpa M. Bangare3

1Assistant Professor, Department of Information Technology, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. ravi.apare@gmail.co
2Associate Professor, Department of Information Technology, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. manoj.bangare@gmail.com
3Assistant Professor, Department of E&TC, Sinhgad College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. pushpa.bangare@gmail.com

ABSTRACT

Advances in information technology and the internet transmission of data have created weaknesses and opened the door to cyber-attacks. In the cloud storage and networking sectors, security and privacy are critical concerns. Cloud computing enabled the internet of things by creating an environment conducive to its implementation. Cloud computing technology included virtual connections to link servers, apps, and other storage devices. Cloud-based data may be edited without requiring significant physical activity. It created insecurity as malevolent people discovered methods to compromise these systems, resulting in intellectual and bodily losses. The report makes many recommendations to address the privacy and security concerns associated with cloud computing and IoT.

The article examines the security risks associated with cloud computing and the Internet of Things in detail. The methodological approach is interpretative.

The findings demonstrate the critical role of machine learning and deep learning in cyber-attack detection and mitigation. To determine the study's reliability, analysis of variance (ANOVA) test statistics are employed.

Keywords: IoT, Cloud, Security, attacks.

I. INTRODUCTION

Without question, the internet of things (IoT) is a paradigm for the twenty-first century. At first glance, the name implies that it refers to linking objects through the internet. This technology was built on a cloud computing (CC) basis; CC devices offer the necessary platform for enhancing and expanding IoT globally [1,2]. Nonetheless, certain security issues continue to stymie the spread of CC-IoT systems into all facets of human life; these worries centre on cybersecurity, with fears about privacy invasion on the rise. Regardless of how advanced technology becomes in areas such as application intelligence and data analytics, the question of how to secure information often arises [3] adequately.

Cloud computing is used by businesses and even the government to store massive quantities of data. Many individuals value the simplicity of use provided by the servers utilized in the procedures. These variables increase the likelihood of malevolent parties attacking and extorting information [4]. Security concerns are a major source of concern for organizations that depend on cloud computing to do business; management of these enterprises asserts that unauthorized actions disrupt normal company operations. Additionally, the risk rises when a business outsources cloud storage services to a provider [5]. Third-party suppliers in cloud computing are a frequent occurrence in the corporate sector; most businesses use them, at least if the vendor suffers from security breaches [6] [7]. With many companies migrating to the cloud, mission-critical business apps and huge amounts of mission-critical data may now reside on systems accessible from any location on the planet. Not only are consumers and workers able to access the system, but also prospective hackers can do so [9]. With the rapid adoption of cloud computing and the proliferation of IoT devices, environmental nuances are also disturbing and altering resilience. The concept of a border is fading away, and the battle against cybercrime has migrated inside.

www.turkphysiotherrehabil.org
The authors addressed vulnerabilities that may result in brute force attacks, Man-in-the-Middle (MITM) attacks, social engineering, and Advanced Persistent Threats, as well as ARP poisoning, firewalls, intrusion prevention systems, and hardware authentication. ANOVA was used to determine the study's reliability. M. L. Bangare et al [25] [26] [27] presented cloud computing work.

The work in this article is divided into several sections; an introduction provides context for the study to be performed, while the second part discusses the background and related work. Section three discusses the research technique, section four discusses the details discussion and lastly, the conclusion discusses the study's research findings and future directions.

II. RELATED WORK

Cloud computing (CC) is changing the way people interact and do business. Businesses still use cloud computing like Microsoft, Google, Apple, and Amazon [10]. The primary impediment to cloud computing's development is data insecurity. Numerous businesses are concerned about the widespread usage of cloud computing in the modern day due to the associated security risk. The data and systems that function on the web are vulnerable to assault by hostile actors [11,12]. The Internet of Things was born when the internet was connected to an embedded computer system that included sensors and actuators. Another description of the IoT comes from Joy's six-web taxonomy, which indicates that the technology falls under the D2D or device-to-device web categorization [13] [14]. Cloud computing and the Internet of Things are inextricably linked. The internet of things enables the linking of smart and non-smart equipment [15]. Cloud computing enables these systems' users to access servers, apps, and other types of storage remotely [16]. Cloud storage may take either on- or off-premise, depending on the service provider and customer. The story reaffirms the inextricable link between the Internet of Things and cloud computing. However, one of these two technologies' drawbacks is its susceptibility to hacking or lack of privacy. This implies that the human customer is mechanically disconnected from privacy and information [17,18]. The internet of things, like cloud computing, has similar security problems. The expanding market for IoT also draws bad actors looking to get access to the industry. These people target the world's vulnerable computers and use them to carry out their illicit operations [19].

The study of the internet of things demonstrates both its advantages and disadvantages, particularly regarding increasing vulnerability, and the ease with which data can be sent back and forth through IoT makes it perfect. Additionally, explain the different levels of the Internet of Things, such as the application and network layers, and examine the particular security concerns that impact each layer. According to the authors, authentication problems exist at the application layer, whereas connection and security issues exist at the network layer. Cloud computing and the internet of things need a technical environment that fits their requirements. According to the article, the Internet of Things (IoT) industry flourishes in the twenty-first century due to its widespread use in various sectors. The Internet of Things is critical for revenue development, cost savings, and monetization of consumer data through value-added services. Cloud computing advancements and diverse networking system applications make it simple to integrate into business processes. This statement demonstrates how the tendency pervades the global economy and plays a critical function in various activities. As a result of this reality, insecurity impacts many businesses worldwide and warrants further attention. Additionally, the Internet of Things improved traditional computer systems defined by their software and implementation. There are six critical aspects to consider when it comes to safe IoT/cloud computing: authentication, confidentiality, redundancy, data freshness, anonymity & abuse, and liability. These characteristics are necessary for a system to operate properly.

The authors addressed vulnerabilities that may result in brute force attacks, Man-in-the-Middle (MITM) attacks, social engineering, and Advanced Persistent Threats, as well as ARP poisoning, DHCP starvation, and countermeasures in their study. Cloud computing's advancements help users on both a business and personal level. The writers of discuss how technology benefits industrial automation and other sectors of the economy. Given that cloud computing established the structural basis for IoT in the twenty-first century, the application possibilities are many. The related work cites a range of sources; they use prototype testing, modelling, and simulation in addition to qualitative information analysis. Antimalware, firewalls, intrusion prevention systems, and hardware authentication were also localized solutions. The business that uses cloud computing should invest in these security measures since abandoning the whole system would be unthinkable given its indicated benefits.
The authors of the article offered answers by examining existing 5G-based systems for CC and IoT and providing an all-inclusive perspective of the structure of these technologies and their associated difficulties. The evaluation focuses on the relationship between the internet of things (IoT) and cloud computing and the current problems and solutions. The research described in [31] delves deeply into the design of network systems and how they are vulnerable to attacks from malevolent people or organizations. The diversity contributes to developing a credible and objective knowledge of cloud computing and Internet of Things security concerns. The findings demonstrate that the technical nature of cloud storage exposes gaps that hostile parties may use to get access to and disrupt a business's operations; these forces businesses to rethink their security procedures and devise new methods of protecting their assets. The majority of these articles emphasize the need of using sophisticated security measures that are often only available to businesses. Individuals will get a better understanding of the advantages of cloud computing and how to safeguard their own devices such as mobile phones and personal PCs via the literature. K. Gulati et al [20] [29] presented IOT and user interface work. S. L. Bangare et al [21] [22] [23] [24] [28] discussed the work in machine learning with scalable issues.

III. RESEARCH METHODOLOGY

The technique makes use of an interpretative approach to information gathering. Numerous case studies, research papers, questionnaires, and expert-led digital interviews will assist in the study and collection of information. Cloud computing security, IoT security, cybersecurity, privacy and trust, problems, challenges, and potential remedies are addressed; certain questions may need an intentional association of IoT with cloud computing. The study methodology is mostly qualitative, using questionnaires, discussions, and interviews to elicit information. The participants will share their experiences with different security solutions and their response to their industry suffers from security breaches. The study goals were outlined, and a questionnaire was distributed to 80 specialists in cloud computing and the Internet of Things. Seventy-five per cent of respondents responded. The following questions are used:

1. How has the incidence of privacy violations changed over the past decade or so?
2. How many data breaches from 2010 onwards can you recall off the top of your head?
3. Weighting of critical variables influencing cloud and IoT application uptake.
4. Consider the following: Do you believe there is any technical solution that successfully reduces insecurity?
5. How can wireless and sensor networks contribute to the age of insecurity's abolition or advancement?
6. Is the business using any human-based security interventions?
7. Is it sufficient for the business to depend only on technical advances?

The interviews assist in resolving the abstract issues surrounding cloud computing and any related area. The structured interview consists of a series of questions covering various subjects relevant to the study goals. The technique enables the interviewee and the interviewer to express themselves freely while examining the issue more in-depth. This study method enables the team to answer the questionnaire's content and see firsthand the feelings and memories connected with the technology. In this situation, case studies include poring through publications on the same subject and examining their findings. This approach enables examining security problems from various angles without becoming fixated on a single area or sector. Case studies offer a more tangible context for the interview findings; they also directly correlate security concerns in the study area. To determine the normality and reproducibility of the data, we utilized ANOVA statistical testing methods using the NCSS data analysis program [32].

IV. DISCUSSION

A comprehensive study is performed to substantiate the research and guide the conclusion. A research approach is created that identifies the variables that affect security models, and their implementation analyzes these aspects and ultimately discusses their effects. In today's technological environment, mobile and online technologies are ubiquitous. All of these developments may be traced back to the internet of things. Experts in their areas promote the development of mobile applications and the supply of quick results to customers. The shift ensures that services are delivered in a timely and convenient manner to residents. Government restrictions and concerns about privacy violations obstruct the work of IT professionals. The load is alleviated via the use of artificial
intelligence methods such as machine learning. The difficulty of regulating such an endeavour appropriately casts doubt on its dependability. When 5G technology is used in industrial IoT to provide superior results, the advantages become practical. The statement demonstrates that technological advancement is critical to modern-day progress.

V. CONCLUSIONS

Cloud computing is a term that refers to technology that enables the virtual storage of data, while the Internet of Things is a term that refers to the connecting of physical objects to the internet. These two technologies are essential in today's corporate environment. The Internet of Things platform developed from the possibilities of cloud computing; both technologies enable businesses and individuals to operate more efficiently. However, the same technologies are insecure; they are vulnerable to hacking and other privacy concerns since cyberspace operates. Complete secrecy is impossible to achieve. Businesses must invest in more robust digital systems and frequently update them to avoid vulnerability. Cloud computing facilitates communication through peer-to-peer connections and is thus very handy for global usage. Individuals with malevolent intents may get access to these same network systems.

As a consequence, information security continues to evolve as an essential component of contemporary technology. Numerous solutions are proposed in the research to address privacy concerns, including anti-malware, firewalls, intrusion prevention systems, and hardware authentication. Anti-malware software is used to protect against viruses, spyware, and other potentially dangerous programs. It reduces the likelihood of malware infecting a computer or network applications. Hardware authentication is another option that works well for cloud computing applications; users must pass through a series of security checks before gaining access to their accounts or databases. The future study may be expanded by gaining access to papers from government institutions and large organizations and enterprise records to improve the precision and detail of the research. Artificial intelligence is a rapidly growing field in the twenty-first century, and it has already been shown to be a viable solution to a variety of global issues, particularly in the security and industrial sectors.

REFERENCES:

29. Kamal Gulati, V.P. Sriram, Dr. Mukta Sharma, Parul, Sherin Eliyas, Sunil L. Bangare, “Use for Graphical User Tools in Data Analytics and Machine Learning Application”, Turkish Journal of Physiotherapy and Rehabilitation; 32(3), ISSN 2651-4451, e-ISSN 2651-446X.