Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/160608

Artificial Intelligence Security Model For Privacy Renitence In Big Data Analytics

S. Saravanan[1,*], *M. Sivabalakrishnan*[2], *N. Duraimurugan*[3] *and D. Divya*[4]

[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology Vadapalani, India
[2]School of Computing Science and Engineering Vellore Institute of Technology Chennai, India
[3]Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India
[4]Department of Computer Science and Engineering, Misrimal Navajee Munoth Jain Engineering College, Chennai, India

Received: 12 Aug. 2022, Revised: 23 Sep. 2022, Accepted: 24 Sep. 2022
Published online: 1 Nov. 2022

Abstract: The smart city uses Information and Communication Technologies (ICT) to build, run and sustain the environment, economic methods to overcome the growing problems of urbanization. Security, security, secrecy and validity have all been important factors in smart city applications, and they are also important in smart city infrastructure interfaces.Hence In this research, an Artificial Intelligence-Big Data Model (AIBM) was developed to enhance the data protection elements of information management interfaces in different smart city applications to address these concerns. A divergent evolutionary method has been implemented in AIBM to provide adequate security for the Secret Data Domain Controller for smart city applications.In addition, the differentiated iterative method has been enhanced by the choice security method based on Big Data Analytics (BDA). It improves the flexibility and dissemination of data in an information authority based mostly on their associated storage site.In addition, ability to adapt interferences approach has been implemented and developed to improve the flexibility and security of information management interfaces in different smart city applications.The reliability of the proposed platform has been demonstrated through computer analysis based on security, accuracy, speed and adaptability.

Keywords: Big Data, privacy, Smart City; Security; privacy; Artificial intelligence

1 Introduction

To improve its efficiency and involvement in community Big Data management, the Smart City idea includes ICT and countless physical hardware connected to the IoT infrastructure. A smart city has been mainly composed of ICT as a framework for developing, applying and encouraging sustainability principles in response to growing urbanized concerns [1]. This ICT system involves a wide range of network devices and machines which transfer information by means of electronic technologies and the Internet.Communities, organizations and individuals could use IoT Cloud applications to collect, evaluate and manage information in real time to make efficient choices that improve quality of life [2]. To maintain the safety and security of large systems, AI and information systems have been embedded in many types of studies to produce intelligent datasets. In addition, several sensors are deployed on AI information management systems, allowing authorities to efficiently organise their local projects. Smart city technology would improve the performance and efficiency of cities in the decades ahead, as the urbanized population continues to grow globally [3,4,5]. To improve the performance and engagement of public database management systems, the Smart City idea includes ICT and many physical devices associated with IoT infrastructure.In database management systems, smart cities around the world should use or plan to use AI for congestion and road crashes [6]. In addition, many monitors have been installed on information management systems using machine learning, which helps authorities to plan their urban projects effectively.

Public health initiatives, which generally describe a series of measures designed to increase certain important characteristics of public services [7], appear to be a frequent practice in health administration. In addition, the policy development process includes some

[*] Corresponding author e-mail: sara.vanan2013@vit.ac.in

non-negotiable conditions that require careful consideration. To begin with, the formulation of 35 health policies requires a multi-stage and continuous procedure that examines Big Data to refine detailed versions and tolerances.Furthermore, the handling of personal health information places strict privacy constraints on both policy formulation and big data analysis [8]. This would be made much more meaningful by the existing EU General Data Protection Regulation 40, which sets out stricter and more precise regulations on the protection of personal information.

2 Related Works

The level of data ingestion is the location where the information was consumed as per the requirements.Screening and surveillance activities or medical records were common sources of information [9]. This would be important information that must be handled according to the rules of international law and rules. It would be responsible for the allocation of resources and the administration of physical and systems services. It is responsible for secure transmission across BDA layers and, if necessary, providing special privacy-related deployments, such as processing and preparing isolated tenants [10,11,12]. There seems to be a variety of BDA available today that includes all of the capabilities from the above levels. Some of these appear to be available through cloud services or software platforms.In this article, humans use the architecture of the Apache Foundation, which would consist of a collection of products and techniques that collectively provide a comprehensive and robust environment.A detailed explanation of the strategy makes it understandable and executable, and ensures that BDA are rolled out semi-automatically and without confusion. Two sets of 245 pieces of information have been used in our BDA public policy approach [13]. On the one hand, information compiled prior to policy development could be used to simulate and projections.On the other hand, information on prospects was gathered while a policy was implemented and used to assess the impact of education policies after implementation [14]. The researchers assume that the retroactive training data set contains information relevant to making a selection, and that this training data set was equivalent to that used in observational research.

Furthermore, the security of sensitive data against unauthorised people was crucial.Smart City People, Governments, Research Organizations, Colleges and Infrastructure, electronic networks ensure that their private and confidential records are protected by proper information security regulations [15]. Apart from data security issues, smart cities face the most difficult challenges in securing the funding needed to expand the concept over the years.One of the most common forms of funding for these financial challenges was personal collaboration [16]. It contributes to spreading early-stage capital engagement by bringing together many smart city entities and participants into a unified network. And promote interoperability in information sharing between government entities and businesses.Government organizations and software developers face important privacy and security challenges [17]. As a result of the already different sensors and the accompanying information management servers.AI technologies have already been advocated as a necessity for the development of smart city infrastructure to handle many privacy and security problems.

The public engagement framework to maximise impact would be a technique for optimizing the impact of social networks in an information-seeking environment [18]. Each user’s impact on the social network was evaluated here.Where the power of influence has been stored on each link, the balanced social network has been safeguarded [19]. Smart cities could use a three-way teaching model to deal with the hierarchical complexity of big data provided by smart cities and also provide multiple levels of data abstraction. Rather than squandering unsupervised learning in improved control methods, the approach leverages a combination of supervised and unsupervised to convergence. By providing multiple-use examples throughout smart city sectors, recurrent neural networks and their transition to semi-supervision would control the intellectual aspect of smart city services & enhance their effectiveness.Relevant studies found that privacy, security, secrecy and validity were important factors in smart cities, and were an important component of smart city information management interfaces [20]. Enhanced government prerequisites, increased demand for advanced services, lower costs and direct connection to automated testing technologies and software. The adaptation of IoT-powered equipment and mobile techniques from formal and informal smart city developers worldwide has driven the global smart city market [21]. In addition, more IoT has been used in the construction of process control in rural and underdeveloped areas. The growth of smart healthcare and smart services has undoubtedly been the main factor in the development of the global smart cities industry[22].

3 Materials and Methods

3.1 AI-Big data Model (AIBM)

Smart cities are a combination of innovative architecture, a networked economy and smart technologies that support growth, family, wealth, learning and enhanced social security.Smart cities would also improve state planning, integrated settlements, development, employment, income, education and social services, and information management systems.If a link to a harmful element exceeds a specific threshold, randomization has been shown to be a success. While a smart city offers additional advantages to its residents, its security and privacy have been compromised due to its reliance on information.Smart Cities were designed to stimulate development, employment, wealth, training and improving social security by combining sophisticated planning, connected communities and advanced devices. Smart cities use new technologies and information to make smarter decisions that contribute to improvement.Businesses can follow the problems to see how industry trends evolve and act with the cheapest and most effective remedies with the most reliable real-time information [23]. Due to inventive efforts, intelligent inventions frequently develop new income-generating technologies.

To efficiently develop a single source of revenue, IoT solutions stimulate cooperation with government sectors and other public service groups.Smart cities, on the other hand, could reduce harmful attacks and facilitate effective asset and urban-wide use. Big data could be used for several purposes as shown in Figure 1. Through intelligent systems and platforms, the building of smart cities produces enormous amounts of information.As a result, the collection of large amounts of data may be a security concern, leading to information leakage or cybercrime. For Smart City implementations, wireless sensor networks frequently support dynamic information sharing and study a multipurpose management technique.The systems rely on Big Data which promotes an ecological, efficient, safe and accessible architecture. Cyber threats and crime do not stand in the way of technological growth or the possibility of making the most of ICT. Smart City applications could track and showcase their global insights in real time using Big Data operating systems. Some Smart City applications might not have been appropriate for the cloud environment [24]. It requires modification in a cloud environment to meet requirements, and the introduction of critical for economic growth intelligence and a better description of information.Several obstacles aggravate the technical issue of digital communities, like unpredictability, high energy, industry hackers, & frontier depletion. Smart cities require a great deal of information to analyze. Solid-state discs have been used by Data Systems in the Cloud to reduce redundant information & encrypt information transit in their datacenters. Cloud solutions generally provide greater financial flexibility than onsite network infrastructure.Smart cities would be crucial in improving the stability and development of global economic growth.

3.2 Mathematical modeling

Security participants often have a high level of trust, but the suspicious encounters were enough to break the trust created.This study offers a technique for evaluating the AI and Big Data model.Registered in xs(x,s) = - 1, the designers find that direct confidence does not affect the assessment.Strategic and organizational decisions could be considered in large data sets.A BDA was used to determine vast amounts of information to identify trends and obtain useful information-gathering techniques.User confidence in security was generally high, but suspicious encounters would be sufficient to destroy the connection between them [25]. BDA in particular, has been used by smart cities to properly acquire and analyze information for a specific location.ICT would help smart cities reduce environmental impacts and use money more effectively.The end-user confidence pattern was defined in Equations 1 and 2 under this system.

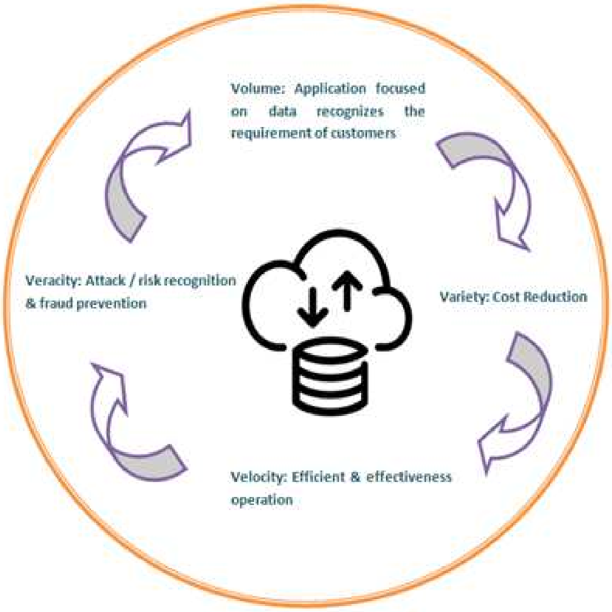
Volume: Application focused on data recognizes the requirement of customers
Variety: Cost Reduction
Velocity: Efficient & effectiveness operation
Veracity: Attack / risk recognition & fraud prevention

Fig. 1: Applications of BDA

$$A_{xs} = \sum_{x=0}^{m-1} e^{x}(1- \in)^{m-x} v_x * sat(x,s) - unsat(x,s) \tag{1}$$

$$A_{xs} = \sum_{x=0}^{m-1} e^{x}(1- \in)^{m-x} v_x \sum_{xesat(x,s)} UX(x) - \sum_{xeunsat(x,s)} UX(\acute{x}) \tag{2}$$

TTo avoid a deceptive rise in malevolent ending customers' sense of security, the normalizing approach indicated in Equation (3) used for end-users confidence.

$$D_{xs} = \begin{cases} \frac{max(0,A_{xs})}{\sum_x max(0,A_{xs})} & if\ \sum_s max(0,A_{xs}) > 0 \\ p_y & otherwise \end{cases} \tag{3}$$

The above-mentioned concept of trust transmission was defined as Equation (4)

$$\left.\begin{array}{c} D_{xs} = \sum_x \sum_{y=0}^{m-1} e^y (1- \in)^{m-y*} A_{xs} \\ w_y = D^{w-ast} D_x \end{array}\right]$$

differential scheme of two level security (4)

The end user inquires about the additional protocol of two different trust enhancements from friends to achieve a wider range of cognitive confidence. As a result, the two-tiered assessment was written as equation (5).

$$\left.\begin{array}{c} w_y = (D^*)^{2*} D_y \\ w_y = (D^*)^{n*} D_y \end{array}\right] \text{differential scheme of one level security} \tag{5}$$

End user x and s treatment process g_{yx} to show finished x's repute, as described in Equation (6).

$$g_{yx} = \begin{cases} \frac{\sum_{q\in com(y,x)} \sum_{y=0}^{m-1} e^y (1-\in)^{m-y*} A_{xs}}{\sqrt{\sum_{q\in com(y,x)} (A_{xs})^2 * \sqrt{\sum_{q\in com(y,x)} (A_{xs})^2}}} & if\ com(x,s) > 0 \\ 0.5 & otherwise \end{cases} \tag{6}$$

End-user A provides the lowest relevant secret to the completed C, as shown in Figure 2. But C has the potential to transcend E's indirect trust. End-users C should have a higher priority for an end-user A than end-users E, which disregards the interests of end-user A.

Improve management and security issues of information management interfaces for various Smart City applications.The decision security system supported by BDA, which can adapt the interference approach, has been designed and created.A Decision Privacy System (DPS) carries out work that could be applied to secure and hazardous processes.

After the introduction of a procedure, the structure changes from condition w0 to w1 with proper coefficients, as shown in Figure 3. At w1, a safe or unsafe approach helps the system deal with the challenge.The system executes tasks if a secure approach has been selected or if it is repeated with a probability of 0.7.If a hazardous procedure is carried out, the software runs the task with the same probability of 0.5.The operation restarts the gadget and restores it to begin w0 in case of malfunction.For example, it is preferable to start with security steps in State 1, then go up to State w0 or w2. Depending on what the opposition is trying to achieve, there may have been different approaches.Every alert signals the co-operation of various parts.To start the process, the enemy chooses the right action and object.

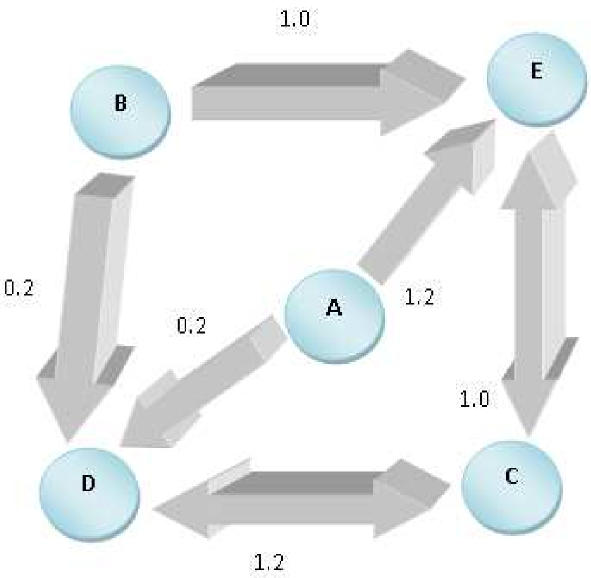

Fig. 2: Information assessment of evaluating trust

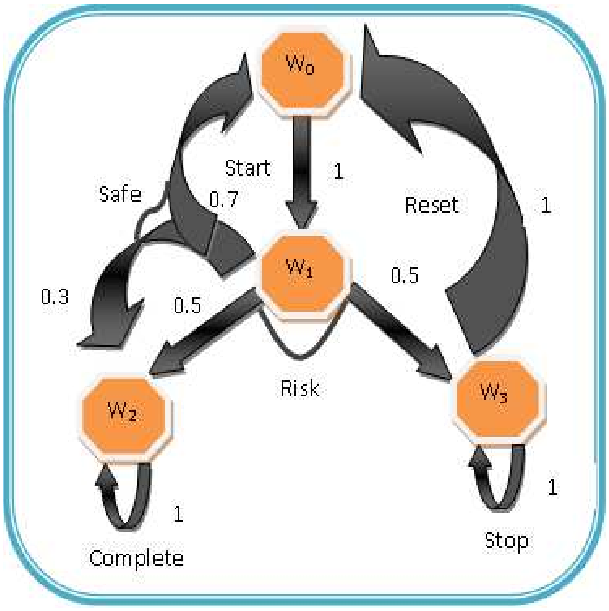

Fig. 3: DPS model

3.3 Privacy management

The Data Privacy & Adaptable Intrusion System was created and developed within BDA to optimize information management interfaces for various intelligent city implementations of scale and privacy issues.DPS serves a function that could be used in the form of secure or hazardous operations. In addition, the Decision Security System for BDA was employed in the differentiated evolutionary algorithms, that detailed account to be increased in terms of processing power & usefulness depending on where it is stored in an information management interface. In order to maximize the information management interface for various smart city applications due to scale and security, flexible technologies are developed and developed.Considering that more of the information collected and analyzed by smart city apps would involve sensitive or private data, most elements of the research and applications must provide an adequate level of security & privacy. While a smart city offers benefits to its residents, depending on their information excessively puts the safety, well-being and security of the city at risk.Unauthorized access to such infrastructure, or malicious attacks, can have serious consequences for city infrastructure, state institutions, and people.The proposed framework validates the organizational image and could even be applicable to a particular arrangement.To mitigate or eliminate the impact of the newly identified weakness, a security officer must update the current configuration...Because the system uses this very same prevent the formation for diverse jobs, the choice secrecy system may autonomously calculate parameters of the model from the learning algorithm, demonstrating its strength & adaptability. The load balance affects the ability, speed of information processing, portability and network management.The load balance between the devices was much smoother if the variation in load balance was reduced. For the computation balancing the load indicated in the following Equation (7) and an adaptive interference technique was used in conjunction with a select security method aided by BDA.

$$LB = \frac{1}{\sum_{x=1}^{M} Y_x} * \left((f_x)^2 . (f_x^p)^2\right) \tag{7}$$

where f_x signifies the service's size, LB means load-balancing data, f_x^p signifies the program's mean allocation of resources, Y_x indicates the energy requirements, & x denotes the number of situations that happened.

The differences between the best and worst responses, and the components, were used to classify the remedies.The optimum response away from the bad has always been the elements that seem to be closest to how to modify.The nearest items along with superior solutions away from the negatives have always been the greatest options.Whenever people open sensitive information through the particular user visited, it is important to ensure that potential attackers are prevented from affecting the user's activity.Experts have developed a set of strategies to protect data and the well-being of the cloud.To enhance the AIBM technique, an integrated ABM method was proposed to reduce client operational burden and eliminate excessively.The successful implementation of the AIBM approach has been adequately monitored.When a user accesses sensitive information, cloud providers use the visited model to stop potential adversaries from insinuating user activity.Experts have explored ways to protect information and improve the wellbeing of the cloud. The strategy guarantees that the information collected has not been misused by unauthorized individuals.The proposed model offers solutions for ongoing security-sensitive pre-assessments and accelerates the collection of evidence, resulting in a significant reduction in image storage capacity.

4 Results and Discussions

To provide reactive activity, real-time updates and control for smart applications were also required.BDA would provide infrastructure services for comprehensive data sets of large smart cities, enabling offline functionality and reduced latency in real-time applications.Security, privacy and authenticity all appear to be important considerations in smart city applications, and they are important in the smart city information management platform.As a result, the aim of this study would be to improve the confidentiality and security of the information methods involved in the different smart cities through the AIBM.The standards focus on large-scale applications and the challenges associated with their deployment in smart cities.

BDA in smart city applications could provide an scalable architecture for huge amounts of information, enabling offline and low latency analysis in practical applications.Offline and low-latency computing may help different areas in a wider ecosystem in practical uses.It helps provide customers with a better experience and products.Better preventive attention, diagnostic and rehabilitation technologies, health information management and medical experience all seem to be attempts to improve healthcare coverage.BDA can be used to significantly improve transport infrastructure routes, adapt them to different demands, and make them more environmentally sustainable.Massive data usage in smart cities requires predictive analytics, which generally require massive computing power.This means hardware and software solutions need to be scalable and reliable.Smart City software must be highly efficient to optimize the consumption of equipment and ensure the smooth running of the many information activities.It shall be performed safely and reliably, as shown in Figure 4, and shall facilitate parallel computing while providing highly qualified group and supplier failure resistance.These technologies manage group platforms to provide an efficient and scalable database for intelligent data applications in communities.

Processing of data in smart cities seems to be more complicated, with numerous process phases involving information gathering from various heterogeneous resources, real-time analysis, & distribution to high-level

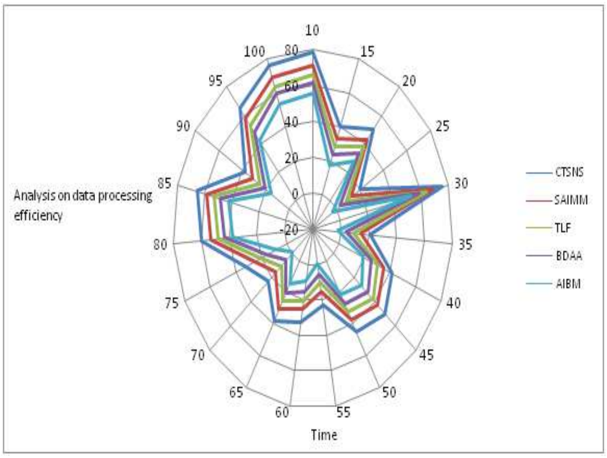

Fig. 4: AIBM efficiency of data processing

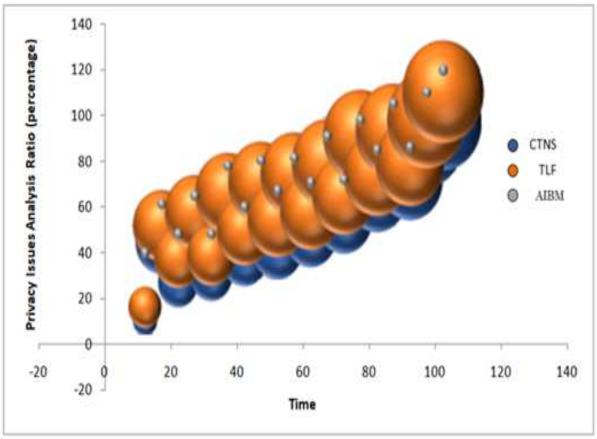

Fig. 5: Smart city analyze the issues

services or applications. In smart cities, the widespread use of information requires data collection, often requiring a tremendous amount of computer power.Scalable and reliable equipment and software were also required.Smart City application software products must deliver the best computer performance, automate equipment usage, and support various data-intensive activities.It eliminates the need for cloud service providers to run dedicated hosting, which is often very expensive, but rather allows them to take advantage of well-developed and highly reliable platforms.Advanced technology has been used by institutions and organizations in smart cities like community outreach societies, health care facilities and the construction sector.Security assessment was most important in smart city development areas, as shown in Figure 5. Security risks include sensitive information exchanged with third-party information and inappropriate communications between AI systems and location information.Developers and consumers have failed to take the necessary and systematic privacy protection measures, as applications with artificial intelligent modelling integrated into Big Data are now rapidly commercialized.

AI technologies use intelligent devices to carry out important activities like automated exchange systems, household items and pacemakers. AI has become more common, creating health risks. For example, telephone suppliers and manufacturers may need information retrieval techniques to identify and retrieve private information that is unrelated to the primary objectives of the solutions.In addition, as illustrated in Figure 6, intelligent attacks on AI have become more prevalent.Hackers might consider how interconnected BDA have been learned or created forever to have a better understanding of the impact of learning and algorithmic performance. BDA plays an important role in analyzing IoT data in a smart city, enabling further research into the city's models and demands.BDA requires the study of large amounts of information to identify models and obtain insights into relevant information. BDA is usually a large amount of information that organizations can use to make business and strategic decisions. BDA would be used to review large quantities of information to identify trends and get an overview of important information.

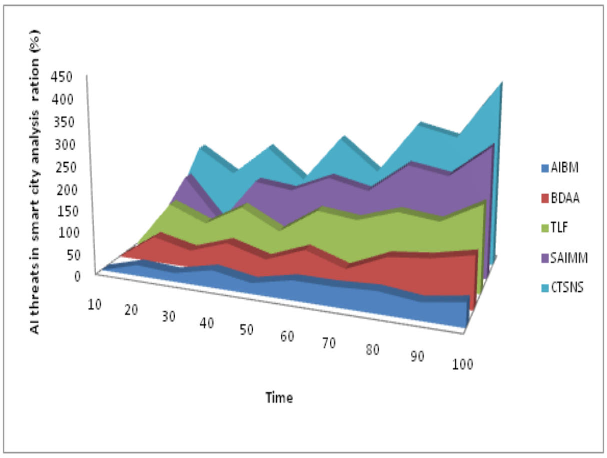

Fig. 6: Smart city analysis over AI threats

The purpose of confidentiality was to protect against passive attacks and access to false data sources.Therefore, encryption techniques have often been used to construct secure communication and storage architectures, ensuring that the transfer of information between nodes remains private.Furthermore, citizen participation would increase the effectiveness of these connected telephones. For instance, early understanding of their safety regulations and concerns would produce the best results in terms of safety tactics.Flexibility has been seen in smart city environments, helping to reduce intrusive attacks. The size of smart cities was exploding, resulting in a huge flow of data and information systems.Consequently, a smart city cannot function properly without flexible processes and procedures.Access generally relates to the ability to access technology and structures upon demand.Smart devices or applications, depending on the subject, should work correctly and during an assault.Also, because gadgets could be attacked, the smart device should discern abnormal changes and inhibit other significant damage.The ability of technology to survive large-scale attacks or tragedies, as well as multiple failures and flaws, was defined as its endurance.Figure 7 shows how the extent of security should have been measured and how to respond to progressively serious threats in an adaptive way.

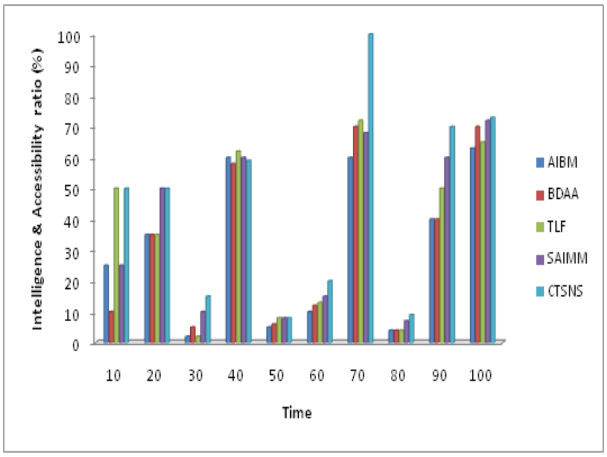

Fig. 7: Comparison of AIBM analysis over existing methods

Accuracy of information would be needed to ensure that data is sent between devices and the cloud.Where information in smart cities could be subject to changes, interruptions, inspections, illegal access, dissemination and cancellation, this procedure was tested.For confidentiality and support, trust, integrity, availability, non-repudiation, security systems and private information, when required. Due to municipal application vulnerabilities, smart city inhabitants may suffer safety & private worries; nevertheless, the public may decline to utilize smart city smartphone applications if they were concerned about safety & privacy.In a variety of intelligent city applications, AIBM enhances the security and confidentiality of information management interfaces.The validity of the proposed application has been demonstrated by computer analysis focusing on safety, accuracy, speed and adaptability.A divergent iterative method was used in AIBM to provide adequate protection for the secret information management interface in smart city apps.A differentiated iterative method was utilized to enhance data scaling & readability based on particular store positions in the data management interfaces, using a decision-making mechanism based on general data gathering. Scalable response methods are frequently designed and constructed to enhance the data management console of various intelligent municipal systems.

5 Conclusion

The growing use of intelligent systems has raised numerous security and confidentiality concerns.It is essential and necessary to build more sophisticated security models and methods in industries and universities.The AIBM method has been proposed to reduce the operational burden of users and eliminate the problem of excessive information gathering.A thorough evaluation of the effective use of AIBMs was performed.AIBM was also chosen to implement the methodology provided for future productions in the actual script of this study.This work have been a process for evaluating the security and confidentiality of services in a smart city information management system to protect sensitive information.

Conflicts of Interest

There are no conflicts of interest declared by the authors for the publication of this paper.

References

[1] V. K. Chattu, A review of artificial intelligence, Big Data, and blockchain technology applications in medicine and global health. *Big Data and Cognitive Computing*., **5**(3), 41 (2021).

[2] A. M. Rahmani, E. Azhir, S. Ali, M. Mohammadi, O.H. Ahmed, M.Y. Ghafour, & M. Hosseinzadeh, Artificial intelligence approaches and mechanisms for big data analytics: a systematic study. *PeerJ Computer Science*., **7**, e488(2021).

[3] Y. C. Yang, S. U. Islam, A. Noor, S. Khan, W. Afsar, & S. Nazir, Influential usage of big data and artificial intelligence in healthcare.*Computational and Mathematical Methods in Medicine*., (2021).

[4] E. Blasch, T. Pham, C. Y. Chong, W. Koch, H. Leung, D. Braines, &T. Abdelzaher, Machine learning/artificial intelligence for sensor data fusion–opportunities and challenges. IEEE Aerospace and Electronic Systems Magazine., **36**(7), 80-93 (2021).

[5] A. Y. R. Al-Shamiri, Artificial intelligence and pattern recognition using data mining algorithms. *International Journal of Computer Science & Network Security*., **21**(7), 221-232 (2021).

[6] A. Chehri, I. Fofana & X. Yang, Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*., **13**(6), 3196 (2021).

[7] M. Bistron & Z. Piotrowski, Artificial intelligence applications in military systems and their influence on sense of security of citizens. *Electronics*., **10**(7), 871 (2021).

[8] S. O. Abioye, L. O. Oyedele, L. Akanbi, A. Ajayi, J. M. D. Delgado, M. Bilal, & A. Ahmed, Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges. *Journal of Building Engineering*., **44**, 103299 (2021).

[9] S. Bag, J. H. C. Pretorius, S. Gupta & Y. K. Dwivedi, Role of institutional pressures and resources in the adoption of big data analytics powered artificial intelligence, sustainable manufacturing practices and circular economy capabilities. *Technological Forecasting and Social Change*., **163**, 120420 (2021).

[10] L. K. Ramasamy, F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi & C. Biamba, Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. *Sensors*., **22**(3), 1076 (2022).

[11] J. Zhang, Reform and innovation of artificial intelligence technology for information service in university physical education. *Journal of Intelligent & Fuzzy Systems*., **40**(2), 3325-3335 (2021).

[12] D. Jiang, *Application of Artificial Intelligence in Computer Network Technology in big data era*. In 2021 International Conference on Big Data Analysis and Computer Science (BDACS) IEEE, 254-257 (2021).

[13] T. P. Latchoumi & L. Parthiban, Quasi oppositional dragonfly algorithm for load balancing in cloud computing environment. *Wireless Personal Communications*., 1-18 (2021).

[14] J. B. Awotunde, E. A. Adeniyi, R. O. Ogundokun, & F. E. Ayo, *Application of big data with fintech in financial services*. In Fintech with Artificial Intelligence, Big Data, and Blockchain, Springer, 107-132 (2021). Singapore.

[15] F. Kitsios, & M. Kamariotou, Artificial intelligence and business strategy towards digital transformation: A research agenda. *Sustainability*.,**13**(4),2025(2021).

[16] V. M. Pavan, K. Balamurugan, & T. P. Latchoumi, PLA-Cu reinforced composite filament: Preparation and flexural property printed at different machining conditions. *Advanced composite materials*., (2021).

[17] P. Garikapati, K. Balamurugan, T. P. Latchoumi, & R. Malkapuram, A Cluster-Profile Comparative Study on Machining AlSi7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. *Silicon*., **13**(4),961-972 (2021).

[18] S. Sunarti, F. F. Rahman, M. Naufal, M. Risky, K. Febriyanto, & R. Masnina, Artificial intelligence in healthcare: opportunities and risk for future. *Gaceta Sanitaria*., **35**, S67-S70 (2021).

[19] K. Zelenak, A. Krajina, L. Meyer, J. Fiehler, E. A. Intelligence, D. Behme & Robotics Ad hoc Committee, How to improve the management of acute ischemic stroke by modern technologies, artificial intelligence, and new treatment methods. *Life*., **11**(6), 488 (2021).

[20] A. C. Bhasha, & K. Balamurugan, *Multi-objective optimization of high-speed end milling on Al6061/3% RHA/6% TiC reinforced hybrid composite using Taguchi coupled GRA*. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)., 1-6 (2020).

[21] D. Dai, & S. Boroomand, A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges. *Archives of Computational Methods in Engineering*., 1-19 (2021).

[22] K. Balamurugan, M. Uthayakumar, S. Sankar, U. S. Hareesh, & K. G. Warrier, Process optimisation and exhibiting correlation in the exploitable variable of AWJM. *International Journal of Materials and Product Technology*., **61**(1), 16-33 (2020).

[23] M. Johnson, R. Jain, P. Brennan-Tonetta, E. Swartz, D. Silver, J. Paolini & C. Hill, Impact of big data and artificial intelligence on industry: Developing a workforce roadmap for a data driven economy. *Global Journal of Flexible Systems Management*.,**22**(3), 197-217 (2021).

[24] T. M. Ghazal, Internet of Things with Artificial Intelligence for Health Care Security, *Arabian Journal for Science and Engineering*, 1-12 (2021).

[25] T. P. Ezhilarasi, N. Sudheer Kumar, T. P. Latchoumi, & N. Balayesu, *A secure data sharing using IDSS CP-ABE in cloud storage*. In Advances in Industrial Automation and Smart Manufacturing,Springer, 1073-1085 (2021). Singapore.

S. Saravanan is currently an Assistant Professor (Sr. G) in the Department of Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India. He completed his B.Tech degree in Information Technology at Anna University, Chennai.He did his M.E in Computer Science and Engineering at Anna University, Chennai.He obtained his Ph.D in Computer Science and Engineering at VIT University, Chennai. He published a number of papers in preferred Journals and chapters in books. His areas of interests include Big data Analytics, Image Processing and Data Mining.

M. Sivabalakrishnan working as Associate Professor in School of Computing Science and Engineering at VIT Chennai Campus since 2013. He has 20 + years of Teaching Experience. He has completed M.E. in Computer Science and Engineering from Anna University Chennai in 2004. He has completed his Ph. D in 2012. from Anna University Chennai. He has published more than 25 papers in International and National journals. His area of Interest is Image processing, Data Mining, Machine Learning.

N. Duraimurugan working as an Assistant Professor (SG) in the Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India. Having 14 Years of Experience of which 12 years in Academic & research and 2 years in Industry. He completed his Doctorate in 2022 at Saveetha Institute of Medical and Technical Sciences, he completed his PG Degree in 2010 at Anna University (MIT Campus), he completed his UG Degree in 2006 at Priyadarshini Engineering College. His areas of interest are Deep Learning, Data Science, Multimedia Technologies, Robotic Process Automation. He has published about 40 International & National and Journal & conferences papers under various domains.

D. Divya is an Assistant Professor in the Department of Computer Science and Engineering at Misrimal Navajee Munoth Jain Engineering College, Chennai,(INDIA). She obtained his Master degree (M.E) in Computer Science and Engineering and Ph.D in Computer Science and Engineering in the year 2012 and 2020 respectively in Annamalai University and Anna University. Her research focuses are Data Mining and Machine Learning. She also published several research papers in referred journals and conferences. She published book title of Theory of computation. She hold 1 patent published under her name.