Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 1, 2020

Review Article

AN ANALYSIS OF ARTIFICIAL INTELLIGENCE IN BIOMETRICS-THE NEXT LEVEL OF SECURITY

ABHISHEK P IYER[1], DR.J. KARTHIKEYAN[2], MD. RAKIBUL HASAN KHAN[3], DR.P.M. BINU[4]

[1]School of Electronics Engineering, Vellore Institute of Technology, Vellore, India. abhishekp.iyer2019@vitstudent.ac.in
[2]Associate Professor, School of Social Sciences and Languages, Vellore Institute of Technology, Vellore, India. jkarthikeyan@vit.ac.in
[3]Associate Professor, Faculty of Humanities & Social Science, Daffodil International University. rakibul.english@daffodilvarsity.edu.bd
[4]ELC, Al-Musanna College of Technology, Sultanate of Oman. binu@act.edu.om

Received: 25.11.2019 *Revised: 05.12.2019* *Accepted: 30.01.2020*

ABSTRACT
In the digital age, security is one of the primary concerns of any organization. Every organization has realized that data is a major resource. Hence, organizations deploy advanced security mechanisms to safeguard business data. However, various industry giants have with major data breaches in the past few years. These data breaches have exposed vital data of millions of customers. Therefore, businesses are constantly looking for better alternatives to traditional security models. Biometrics such as fingerprint and iris scans are being utilized for authenticating employees at the workplace and identifying smartphone owners. Such biometrics can be implemented in organizations to authorize data access for confidential data. Biometrics can be used along with traditional passwords or PIN numbers for multi-factor authentication. Additionally, the adoption of AI will help develop data-driven security protocols. Hence, clubbing AI and biometrics together will lead to the creation of dynamic security models.AI systems can minimize' human error ' events, provided they are properly programmed and can contribute to making quicker choices through cognitive techniques. It is considered to be a very effective technology as it challenges the hackers to penetrate and ensures safety among the users.

Keywords: Next Level of Security, Artificial Intelligence, Ensures Safety.

DOI: http://dx.doi.org/10.31838/jcr.07.01.110

INTRODUCTION

Biometrics literally means "*life measurement*". Biometrics refers to any reliable method that differentiates one person from another using measurable qualities that may be physiological (fingerprints, hand geometry, retinas, iris, facial image) or behavioural (signature, voice, keystroke rhythms). These examples are a few among the many methods employed in today's world. In practice, all biometric systems run on a common principle that unfolds to a two-step process. The first step is Enrolment, in which new users are added to the database by recording their data for the first time. Information regarding a user is captured that is then sent through an algorithm that turns this raw data into a template which will become a part of the database under the user's data. We must understand that it is the template that is stored in the database not the actual data, and the template contains very little data in the form of digits. The second step is Recognition. When a data is entered for recognition, it's converted into a template using the same algorithm mentioned above. This template is matched against the database and if it's either a positive or a negative match it's indicated accordingly.One must understand that there is a difference between authentication (confirming someone's identity) and identification (finding someone's identity), the key difference is that authentication is a one-to-one verification while identification is a one-to-many verification.

Some of the many applications of Biometrics include –

- Military – Every military in the world has an established department for data and information security, biometrics find their use in this field helping safeguard secrets, prevent imposters and provide an ease of access to retrieve information when the organisation sees fit.
- Biometric Passport – Minimises passport fraud and forgery, some passports contain RFIDs which help in further facilitating the identification of an individual.
- Airport security – Ben Gurion International airport in Israel, being one of the busiest airports, it implemented biometric kiosks which enabled smooth functioning without much delay and also minimises human error among other factors.
- Financial Transactions – All modern ATMs are equipped with fingerprint scanners, facilitating card-less transactions.

Biometrics finds their use in many fields of everyday hustle, but there are many areas in which it lacks the required specifications,

- Security is one of the foremost reasons, biometrics are secure but they are not totally fool proof. Since it matches with records, databases can be hacked into and can be tricked into making it look like the biometric is entered.
- Twins can beat facial recognition.
- AI can beat standard biometrics by deceiving it using synthetic fingerprints. Brute force attacks can be orchestrated with such synthetic fingerprints, trying every option till none are left.

Since AI can beat classic biometric devices, what better way to develop better biometric devices than to integrate the very threat and make it the sharpest arrow in it's quiver. AI integrated with biometrics can increase the security and consistency by a thousand-fold

LITERARY SURVEY

Boukhris, M., et.al.(2011) This work deals with how facial recognition can be applied to virtual avatars. Avoiding fraud in multiplayer online games is a point of concern and this helps in eliminating this threat to a certain extent. The researchers used a couple of techniques like, SVM (Support Vector Machine) and Wavelet transformation. SVM learning machine works as a discriminant or a classifier and with the help of wavelet transformation's features it's efficiency is highly increased. Wavelet transformation finds it's use in image processing and in the research conducted it was mainly used for characterization. Object recognition is being achieved by SVM machines which when integrated into the said machine can help characterize digital avatars in no time. Classification of facial expression is a new challenge faced by the SVMs. It's basic functioning can be elucidated as the following, the data it takes in is rearranged into a form readable and understandable to the program using a global algorithm. The system performance is estimated by measuring two error rates: FAR (False Acceptance Rate) and FRR (False Rejection Rate). In the above experiment, the data indicates that the average FAR rate is 5.5% and FRR is around 2% (The exact data was removed). This is a massive improvement when compared to standard biometric checks. This method has limited to 10 images per entry, it was sufficient since avatars have very low number of facial expressions, but when applied to humans, the resolution and data collection must be more quantitative.

Purgason, B., & Hibler, D. (2012) Usage of AI and neural nets to analyse KIT Biometrics (Key Interval Time). KIT is an attribute of a person that is not easy to wilfully and precisely tamper. The standard keyboard is divided into 10 word-groups that are assumed to be the different keys the 10 fingers would hit. URIEL (User Rights and Integrity Enforcement Logic platform) was devised for the purpose of using neural nets to analyse KIT. During the first human trials which were anonymous, URIEL was allowed to either refuse or make a decision judging by the confidence of the answer. URIEL could make a decision in 82.178% of the cases but not in the rest. Indicating that, URIEL would rather not make a comment than make a wrong one, which tells us the integrity and surety of the correctness of the answer. Each individual entry when added to URIEL increased the accuracy of the result. URIEL uses the KOH (King Of the Hill) methodology, that is the most powerful positive entry is declared as the winner when there are multiple entries, in a case when there are no positive entries, URIEL fails to make a decision. The data collected indicates that URIEL will make a correct decision more than 82% of the all given entries and does not give a wrong indication more than 2% which is a very promising result in the field of biometrics. Less than 18% of the entries, URIEL refuses to make a decision which can be improved in further calibration. The key point we need to understand here is that AI has a strong potential in behavioural biometrics.

Kalera, M. K., et.al. (2004) Offline signature recognition, online signature recognition is more dynamic as it shows the path which the subject used while putting a signature. This can help to some extent eliminate forgery but skilled forgers can bypass this too. In offline signature recognition the stroke of the signature is not very easy to determine. Signature is a behavioural trait that is obtained by the continuous practise over a long period of time, it is not a psychological biometric. During the research two databases A and b were considered, A is a total offline database where signatures were scanned in 256 shades of grey and exported in a PNG format, while B is a digital database of signatures. Since database B was a digital one, first the pen coordinates had to be transformed X-Y coordinates, which took a long time in pre-processing. The signatures were passed through a system of GSC features, i.e. Gradient, Structural and Concavity. It converts the signatures into a binary format and compares two using similarity measure. Two thirds (16) of all the signatures of each writer were used for training, while the rest (8) were used for testing. The results for database A and B are measured by plotting a graph between FAR (False Acceptance Rate) and FRR (False Rejection Rate). The ERR (Equal Error Rate) for Database A was 21.90% and B was 32.37%. For a purely offline system, an accuracy of 93.18% was obtained, integration of DPW (Dynamic Plane Wrapping) with this method can increase the efficiency of the technique many-fold.

Lanitis, A. (2009) Aging considerably affects the face of an individual for obvious reasons, it is natural and irreversible. Researchers in this field are trying to define facial biometrics in such a way that recognition is not hampered due to aging. Aging affects individuals on different levels, some start showing the traits of aging very early, some do not even after a long time. The point here is, one cannot define a common aging pattern that is applicable to all subjects. We define two groups A & B and C &D, where A & B have an average age difference of 1.6 years and C & D have an average age difference of 15 years. The conclusions derived are that a drop in efficiency of 12% is noticed when dealing with different age distributions. Also, the upper region of the face is more prone to rejection after aging than the lower face region. Since we already established that effects of aging come about in different individuals on different basis, Data driven research in this area is of no use. This can be bypassed only by the use of smart systems which are capable of modifying the facial templates taking into consideration the parameters of aging and also that the template is consistent with the current visage of the individual. This is very tedious and seems somewhat impossible since the external factors affect the process of aging and cause compounded results. For this sole reason usage of a state-of-the-art AI system is highly beneficial in facial recognition. A system that takes into account the possible affect of external factors and at the same time, a definition of facial representations that include discriminatory as well as time invariant features is the need of the hour.

Kocher, R. W. (2006) C-BAD (Cooperative Biometrics Abnormality Detection system). Through the usage of C-BAD one can effectively monitor an individual's activities and any anomalies if detected, will be automatically reported to the security personnel. Organization are well equipped for external threats, but internal trust issue is something an organization is not properly prepared for, employers cannot effectively visualize their employees as threats, which is where corporations are viable to be maliciously harassed. If employers view their employees as potential threats, a peaceful work-place environment cannot be established. In an analysis of 100 information security systems, 45% were malicious, 10% were criminal. One out of every two of these people were information technology professionals, and 19% of these were top-level system administrators and 31% of those turned out to be assistant system administrators. Insiders can only be caught if the evidence is over-turning, else none of the co-workers would testify to the possible crimes of one of their own. Some of these abnormalities might look like, working after/before scheduled work hours, making copies or printing or access information that is not authorized to them. Classified files of an organization are not tracked in this manner, since tracking requires giving C-BAD full access to the files and sensitive information cannot be made open to any other person. C-BAD's main access rests only with the head of the organization and the main computer server is embedded with AI or a rule-based system, which decides whether an abnormality is worth pursuing or not, eliminating the human element thereby maintaining complete integrity and publishing an unbiased result free of any persuasion.

Yao, Y. F.,et.al.(2007) The typical BA (Biometric Authentication) shows three characteristics: large number of individuals, small sample size, high dimensionality. A major issue in BA is single sample biometrics recognition problem, where only one sample is provided which must be used for future authentications. This

often leads to a bad recognition rate. Here, a better approach based on feature level biometrics fusion is presented, where two types of biometrics i.e. Face feature (A contactless biometric) and a palm feature (A normal contact biometric). The discriminant attributes are extracted using Gabor-based image pre-processing and PCA (Principal Component Analysis) methods. That means, the defining features of an individual on these two fronts are separated and are stored as the recognition data in the database. After this, a distance-based separability weighting strategy is developed to cause feature level fusion. Usage of a large database for face and palm significantly improves the recognition rate, which is expected, as vaster the database the program is provided with the more defining features or differences it can import into the recognition database. This helps countering the hindrances in single sample biometric and enhance the performance of BA system. It also indicates that there is a strong correlation between face and palmprint biometrics.

Boult, T. E., et.al. (2009) In Biometrics, Geometry identification methods identify the person using the geometry of a sub region of the said subject. Hand geometry identification rests on the fact that each person has a reasonably different hand shape and it does not change after a period of time. The shape of the hand alone might not be able to differentiate people all-together, therefore it is necessary to define other attributes too. To effectively distinguish two hands to the precision of the highest order, the pictures of the individual hands must be taken from the same distance and the same angle with respect to the hand. This must be taken care of during the enrolment process itself. For verification, it is understood that comparison takes place on a one-one basis, but during Identification, it is crucial that the subject is compared with each entry in the database. This program combines the planar projective invariant features, obtained from the hand biometric with the traditional biometrics derived from the facial recognition. The key point here is that, both of these features can be captured in one image, which makes storage hassle-free and reduces the amount of data wastage during Enrolment, this not only facilitates storage of a large database of individuals but also does not hamper the recognition on any evident level.

Wong, F. W. M. H., et.al. (2001). Increased use of technology has presented us with many advantages, but one of the disadvantages is balancing both security and accessibility. Keystroke dynamics rely on two outputs, one is Verification (Am I who I claim I am?) and Identification (Who am I?). Usage of this technique with pin or password protection increases the efficiency. The intruder must not only know the password but also the rate at which the password is typed-in by the user. This type of biometric is very economical without reducing the security. Usage of a RTC (Real Time Clock) or CTC (Clock/Counter Time Chip) is viable for the time interval system. This program developed in visual C++ uses K-Nearest Neighbour rule classify data, the unknown input data is assigned to the nearest neighbour in the series, this might seem like it will decrease the integrity of the system, but at the resolution at which each data set is stored, KNN(K-Nearest Neighbour) will have no effect upon the security of the system but it will certainly reduce the recognition time which is a very useful feature. ANN-MLP (Multi-Layer Perceptron for Artificial Neural Networks) is another mechanism that can be employed. The average authorized acceptance rates and False acceptance rates are 84.63% and 1.03% for KNN and 99% and 29% for ANN-MLP respectively. Which method to employ solely depends upon the choice of the user.

Mazouni, R., &Rahmoun, A. (2011) This work talks about fusion methods, integrating more than one biometric data of an individual to facilitate better recognition. The 5 decision level schemes that are generally used are, BFS (Brute Force Search), PSO (Particle Swarm Optimization), SVM (Support Vector Machines), ANFIS (Adaptive Neuro Fuzzy Systems), GA (Genetic Algorithm). The results are calculated with and without applying normalization using UCN (Unconstrained Cohort Normalization) and the performance is noted using EER (Equal Error Rate). Each of these methods specialises in its own way of combining data and reviewing them, each of them performs differently under different constraints and situations. Comparing one another could be a very illogical approach but under ambient conditions, the comparisons could make perfect sense to those who understand data. The results are as follows, GA and PSO outperform other methods due to their strength of scanning a large database. ANFIS's results are close to that of GA and PSO due to the usage neural networks to obtain the suitable parameters to get the best Fuzzy Interface System. SVM has the worst performance owing to the fact that the genuine distribution and imposter distribution have a lot of intersection.

Koppel, M., et.al. (2004)Text categorization for authorship verification. In the classical method, the text of an author is scanned and 200 of the most used words are taken and are deemed content words and are removed manually and the rest of the words are taken into consideration and are compared. But using AI, each response is taken as a vector of dimension 130. Each entry of this vector represents the relative frequency. Then a variant of an exponential gradient is used to distinguish between different collections. This is a different kind of biometric, one that is not often used. But many of the plagiarism software use this technique. To a layman, this might seem as a not so useful kind of biometric, but many lovers of literature around the world will agree plagiarism is no less than a crime that one can be convicted for. AI streamlines the process of "unmasking" which is separating the best discriminators and distinguishing the work finding out the penmanship of both, standard algorithms cannot effectively outthink the creativity of a human mind but a digital mind if not outsmart is capable of at least drawing comparisons between two works.

SudhirBabu(2019) Artificial intelligence plays a major rolein our daily life of the growing workforce and its increased availability revenues. The banking industry now is one of the most significant industries in India.Worldwide, banks undergo fast digital transformation today to strive for higher advantages, for example, improved synergy, cost savings, corporate effectiveness, mitigate cyber hazards, etc., and the latter is among the top priorities. Due to the huge volumes of money and consumer information banks, it has become a top goal for hackers. As frequent headlines of information infringements indicate, banks face constant threats of economic loss, regulation and reputational damage. In addition, fraud has spurred bank staff and clients alike to force banks to multiply their safety architectures. There can be no doubt that banks and financial institutions need to be cyber-safe from the inside. In the years since the emergence of the Artificial Intelligence (AI), physical signatures have been superseded by contemporary biometrics and further developed.

Chris Burt(2019)Huawei is the biggest provider to NEC (serving 14 nations) for 50 nations, much more than any other business.Just over half the "developed democracies," as opposed to only 37 percent of autocratic States, use AI monitoring systems; but the research also notes that the systems are not necessarily abused.

Jack Corrigan(2019) Ultimately, according to the Intelligence Advanced Research Projects Activity, the CIA's study group, the tech would allow spy organizations to identify quickly individuals who use cameras installed on far-off rooftops and unused planes.Facial identification and other kinds of biometric technology have considerably enhanced in latest years, but even today's most sophisticated technologies are less reliable and have no clear vision of their topic. Even if the individual stands nearby and sees the camera straight, the facial identification technology may be susceptible to mistakes. However, the

intelligence community tries to overcome these constraints in two ways: by collecting further education and by developing systems based on various data types that identify persons.

Steven Feldstein(2019) The technology of artificial intelligence (AI) is fast spreading worldwide. Beginning with profound videos which blur the line between reality and falsehood, innovations continue to emerge and sophisticated algorithms can battle the finest players in multi-player poker in the globe. Companies use AI to enhance analytical processing; town authorities use AI to monitor traffic jams and to monitor intelligent energy measuring.Yet an increasing number of nations are employing sophisticated monitoring instruments for the monitoring, monitoring and monitoring of people in order to achieve a variety of policy goals- some legalizing, some violating human rights, and many of them in a dark middle ground.It is essential that we first know where these instruments are implemented and how they are used to properly tackle the impact of this technology. Such data is unfortunately limited.To make matters clearer, this article provides an AI Global Monitoring Index (AIGS), a first of its kind in studies. In 176 nations around the globe, the index compiles empirical information on AI surveillance use. It does not differentiate between lawful and illegitimate uses of AI monitoring. The aim of studies is instead to demonstrate how fresh capacities to monitor and track people or systems transform the capacity of governments.

LuanaPascu(2019) All over the world customers use digital platforms, including banking transactions, for everyday activities. The world is in the middle of a digital revolution in banking and the Fintech environment, which offers solid safety, a better mobile banking experience, economic growth and innovation like biometric technology and digital identity.The concern of the GCC's banks is that financial transfers, foreign exchange services, and payment services will be revolutionized by FinTech firms in order to reduce transfers and time. According to S&P, the traditional banking and exchange activities in GCC could have a big effect in this respect.However, it is clients and not so many regulators who are pressuring the sector for more efficient service delivery. In understanding the strength of strategic partnerships, regulators support banks working with FinTech firms to provide their clients with optimized and safe alternatives.Until recently, hackers had only used their personal identification numbers in the region to facilitate taking over their accounts. The fresh approach comprises in the combination of biometric identification, most probably in the form of finger print scanning, passwords and individual identification numbers, which is, according to Banking CIO Outlook. By implementing biometric authentication, APAC banks are not only interested in reducing traditional banking expenses, but want to also provide improved user experience and enhance safety. One option is a subscription-based Biometric-as - a-Service (BaaS)

Alex Willis(2019) Biometrics may sound futuristic for the uninitiated, but you probably already use these solutions. The "Future of Identity" research by IBM Security shows that biometrics— the uses of technology to identify and regulate access based on one's own biology— are fast becoming commonplace. Almost two thirds of participants say that biometric authentication, such as fingerprint or facial awareness, today is convenient, while over 87% say that they will use those techniques very comfortably in the very close future. Biometrics alone is not enough to 100% secure hackers from economic data and information. In addition to smart safety, however, the combined findings are almost impenetrable. The application of artificial intelligence and machine learning methods to financial safety systems lets the customer learn how legitimate users interact with their financial services, making it simpler to identify and identify unorthodox trends and behaviours. This kind of analytical safety uses algorithms to know more and safeguard the user based on his past / typical behaviour. In addition, local information can be used to further protect customers against economic fraud and assault in their patterns of behaviors and usage. When a login attempt is made outside its ordinary place (i.e. home, place of work, or residence) on your mobile phone, for instance, this can be flagged as suspicious activity instantly as possible. However, AI can use the information provided by your financial institution to conclude that the suspected flag of activity is wrong if you know your financial institution is visiting another town because it processed your air ticket's transaction. Even when a customer usually accesses his account or conducts his or herself on a day or days of the week

Inge De Bleecker(2019) Here's Artificial Information (AI). In many sectors, the technology already has an effect. IDC estimates that global AI systems expenditure in 2019 will reach $35.8 billion— a 44 percent rise compared with 2018.It's time to start up for every company which hasn't began its AI voyage. This is because AI shakes up its client experience and brings consumers and brands closer than ever. However, many individuals have not yet understood or understood the application scope of AI. Three methods are already affected for millions of customers by artificial intelligence. CX.When thinking of customisation, Amazon and its huge inventory of products for purchase is one of the first things to remember for many. Based on their known preferences and buying history, customers are supplied with personalized suggestions. This bit of AI support enables shoppers to discover the needle in the haystack: the things they are looking for in the millions of accessible goods. It enables Amazon, the retailer, to secure a sale.In common smartphones and many FinTechn applications the science of biometric identification is already being applied. Apple's Face ID enables consumers to easily unlock their phones by looking at it. Fingerprint readers are integrated into Smartphones and laptops. However, some businesses go beyond smartphones and laptops to have a fresh effect on client experience.

LuanaPascu(2019) Singapore retail businesses Octobox, OMO Store and Pick & Go have lately announced the strait times at Singapore Retail Industry Conference and Exhibition that a increasing amount of convenience shops should accept the idea until the end of the year.m Deployments, such as palm scanners, allow the buyer to enter the kiosk, RFID tracks the purchased items and AI tracks movement inside the kiosk. Smart cameras and intelligent racks will be used as well as these characteristics to enhance the travel and experience of buyers in data analysis. Retail industry is confronted by a absence of staff and serious competition from internet distributors and is suffering from "downside hazards and the many worldwide uncertainties," Chan Chun Sing, Minister of Commerce and Industry at the case explained. Singapore retail businesses hope to overcome the hard times with innovation by creating a notion from the Enterprise Singapore government agency."They demonstrate the sector's spirit to be continuously innovating and testing fresh alternatives even in challenging times," said Chan Chun Sing, Minister of Trade and Industry.

Chris Burt(2019)The new AI engine improves the biometric fingerprint efficiency of MorphoWave Compact. According to a business announcement, Idemia has added to its MorphoWave Compact touch-free, 3D biometric fingerprint terminal, fresh artificial intelligence capabilities, considerably enhancing end-use experience and efficiency. Last year's MorphoWave Compact was introduced with an 86% less footprint than the MorphoWave Tower for highly-voluminous biometrical scans. Idemia reports that the new AI-based integrated biometric motor enhances matching velocity by 85% with a rise of 25% to over 50 individuals per minute at each point of access. The algorithms also improve match precision and allow for one-to - one identification capacities of up to 100,000 users. In addition, the firm claims that the new AI capacities assist the most demanding MorphoWave Compact fingerprints. Idemia Connected Objects Executive Director Yves Partalier remarks: "Technology is

evolving at an incredible pace and it constantly challenges and redefines client practice. "Innovation is part of our DNA at Idemia, and pushing the frontiers. This recent innovation represents yet another step forward in biometric identification and enables us to stay a leader in the field of increasing identity.

Chris Burt(2019) Progress in Nigeria and airport biometrics technologies make up several of Biometric Update's most common papers this week, and we recommend reading for those who live and work in and around the sector for a few comparatively thoughtful reviews of AI-related questions, in specific facial recognition. One of the more widely read stories about biometric update this week are a couple of significant announcements regarding Nigeria, which have borne remarkable results in their involvement with the global identity community. The National Identity Number (NIN) program for Nigeria will be extended to nearly 100 million people in the next three years by $433 billion, and the country has declared 16 September National ID Day in the heels of that announcement.Worse, there have been several tales of profound fraud that will promote concerns (and positions) that tech and AI in specific are out of control and need to be regulated. Although most depths are detectable by biometrics and other technologies, developments in AI may not be the case soon, according to the inside BigDATA editorial. In the commentary on Dark Reading, Shape Security CTO Shuman Ghosemajumder reports that the continual threat to private information and data in particular which could fuel deep fakes or more traditional cyber-threats is a straightforward money collection, yet it may get better.

FINDINGS

The findings could be summed up to be the comparison between different methods used for integrating AI with biometrics. In the field of biometrics, measurement of success of a technique is done by measuring two parameters, FAR (False Acceptance Rate) and FRR (False Rejection Rate).FAR meaning if the biometric machine gives access to someone who isn't in the database, in other words someone who shouldn't be able to access it. FRR refers to the system denying access to an authorized individual. Each of the above research work indicates with the data that biometric system works better with AI. While the real question remains, which method to employ while integrating biometric and AI, some of the fusion techniques spoken about in the Literary survey number 9 talk about combining different data types to a single one, so that the neural nets can effectively work there on. Of those two methods GA and PSO outperform others, due to the method employed to merge the data belonging to one individual. Hence, we can understand from this that there are various methods that can be used but to determine which is better suited for the operation in question, through research must be done.

In the years since the advancement of Artificial Intelligence (AI), physical signatures have been replaced by modern biometric and further developed. Using AI, behavioural abnormalities can now be monitored and safety threats can be prevented much more precisely. With this technology, the operations of bots and hackers are now simpler to recognize. The Intelligence Community is Exploring Long-Range Biometric Identification. Technology of Artificial Intelligence (AI) is growing quickly worldwide. The launch of deep videos blurring the line between reality and falsehood is continuing to lead us to sophisticated algorithms, which are the finest players in multiplayer poker on earth.

AI and intellectual science are two unmistakable orders, with covering techniques yet with rather various objectives. Artificial intelligence is a part of software engineering and is worried about the development and arrangement of savvy specialists as PC programs, and furthermore with understanding the conduct of these ancient rarities. The center logical objective of AI is to comprehend the fundamental standards of wise conduct that apply similarly to creature and fake frameworks. Practically the majority of the work is numerical or computational in character and a significant part of the writing is procedure situated.

Psychological science is an expressly interdisciplinary field that has support from AI, yet in reasoning, brain science, and subfields of other social and organic sciences. The binding together objective of intellectual science is to comprehend and show human knowledge, utilizing the full scope of discoveries and systems of the integral orders. As one would expect, a wide scope of methods from the scientific, conduct, social, and natural sciences are utilized. There are research bunches that are dynamic in both AI and psychological science, yet they will in general produce various kinds of reports for diaries and gatherings in the two zones.

CONCLUSION

Biometrics are a daily part in many of our lives from unlocking our smartphones to marking our attendance, even the government of India identifies individuals based on their biometrics enrolled during their Aadhaar enrolment. All of this points to the fact that biometrics are already in use, the need of the hour is to improve the present technology so as to facilitate the working of these machines in a more effective way. Faster and More secure, it can be achieved through the use of Artificial Intelligence. Neural network, Machine Learning, Data analytics all of these are branches of AI and each of these play a vital role in improving biometric technology. Today's biometric machines are not capable to withstand brute force attacks. After going through many research stories, what I understood is, there is a lot of effort going into testing various methods for increasing the safety of biometric machines but these results are not reaching the scientific community on such a level where they can produce a lot of impact and even if they are, technical giants are not very comfortable in adding AI as an element into their appliances, since a majority of the customers do not yet totally what AI is and what it is capable of. As many advantages as AI has, there are only so many flaws, a lot of research has been done and is being done and I'm sure will be done too, to overcome these challenges. The next biggest challenge would be taking this to technology to a layman, which is a task easier said than done.

Large businesses were victims of violations of safety, which affected e-mail addresses, private data and passwords. On a number of occasions, cyber safety specialists have repeated that passwords are highly susceptible to assaults, private data compromising, loan card data and social security numbers. All this is why biometric logins contribute to cyber safety in a beneficial way.

Technology has made our lives really simple, particularly artificial intelligence. Even without knowing when we did it, the overall applications to Alexa have entered in our houses technology. Here is an easy look at how AI will play a major part in every stage of our lives.

Continuous equipment maintenance is an enormous cost to producers, and the move from reactive to predictive maintenance has become a must for every manufacturer. AI has managed to save business time and money by using sophisticated AI algorithms and artificial neural networks to predict asset malfunction and briefing engineers in advance.

REFRENCES

1. Alex Willis(2019) Using Biometrics, Intelligent Security To Keep Finances Safe, derived from https://securityboulevard.com/2019/08/using-biometrics-intelligent-security-to-keep-finances-safe/
2. Boukhris, M., Mohamed, A. A., D'Souza, D., Beck, M., Amara, N. E. B., &Yampolskiy, R. V. (2011, July). Artificial human face recognition via Daubechies wavelet transform and

SVM. In 2011 16th International Conference on Computer Games (CGAMES) (pp. 18-25). IEEE.
3. Boult, T. E., Zheng, G., & Wang, C. J. (2009). U.S. Patent No. 7,623,685. Washington, DC: U.S. Patent and Trademark Office
4. Chris Burt(2019) Carnegie report says facial recognition and AI surveillance spreading faster than thought, derived from https://www.biometricupdate.com/201909/carnegie-report-says-facial-recognition-and-ai-surveillance-spreading-faster-than-thought
5. Chris Burt(2019) High traffic identification tops this week's biometrics and digital ID news, derived from https://www.biometricupdate.com/201909/progress-in-nigeria-and-high-traffic-identification-top-this-weeks-biometrics-and-digital-id-news
6. Chris Burt(2019)New AI engine boosts MorphoWave Compact biometric fingerprint performance, derived from https://www.biometricupdate.com/201909/new-ai-engine-boosts-morphowave-compact-biometric-fingerprint-performance
7. Inge De Bleecker(2019) 3 Ways Artificial Intelligence Is Transforming Customer Experience, derived from https://www.cmswire.com/digital-experience/3-ways-artificial-intelligence-is-transforming-customer-experience/
8. Jack Corrigan(2019)The Intelligence Community is Exploring Long-Range Biometric Identification, derived from https://www.nextgov.com/emerging-tech/2019/09/intelligence-community-exploring-long-range-biometric-identification/159907/
9. Kalera, M. K., Srihari, S., & Xu, A. (2004). Offline signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence, 18(07), 1339-1360.
10. Kocher, R. W. (2006). U.S. Patent No. 7,028,018. Washington, DC: U.S. Patent and Trademark Office.
11. Koppel, M., Schler, J., &Mughaz, D. (2004, January). Text categorization for authorship verification. In Eighth International Symposium on Artificial Intelligence and Mathematics. Fort Lauderdale, Florida, http://rutcor. rutgers. edu/~ amai/aimath04/SpecialSessions/Koppel-aimath04. Pdf.
12. Lanitis, A. (2009). Facial Biometric Templates and Aging: Problems and Challenges for Artificial Intelligence. In AIAI Workshops (pp. 142-149).
13. LuanaPascu(2019) Banks in GCC, APAC adopting digital identity, biometrics, AI, derived from https://www.biometricupdate.com/201909/banks-in-gcc-apac-adopting-digital-identity-biometrics-ai
14. LuanaPascu(2019) Unmanned stores using biometrics, artificial intelligence to be tested at Singapore university campuses, derived from https://www.biometricupdate.com/201908/unmanned-stores-using-biometrics-artificial-intelligence-to-be-tested-at-singapore-university-campuses
15. Mazouni, R., &Rahmoun, A. (2011). On Comparing Verification Performances of Multimodal Biometrics Fusion Techniques. International Journal of Computer Applications, 33(7), 24-29.
16. Purgason, B., & Hibler, D. (2012). Security through behavioral biometrics and artificial intelligence. Procedia Computer Science, 12, 398-403.
17. Steven Feldstein(2019) The Global Expansion of AI Surveillance, derived from
18. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
19. SudhirBabu(2019) How AI & biometrics have changed the face of Fintech sector, derived from
20. https://www.analyticsindiamag.com/how-ai-biometrics-have-changed-the-face-of-fintech-sector/
21. Wong, F. W. M. H., Supian, A. S. M., Ismail, A. F., Kin, L. W., & Soon, O. C. (2001, November). Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. In Conference Record of Thirty-Fifth Asilomar Conference on Signals, Systems and Computers (Cat. No. 01CH37256) (Vol. 2, pp. 911-915). IEEE.
22. Yao, Y. F., Jing, X. Y., & Wong, H. S. (2007). Face and palmprint feature level fusion for single sample biometrics recognition. Neurocomputing, 70(7-9), 1582-1586.
23. Gangurde HH, Gulecha VS, Borkar VS, Mahajan MS, Khandare RA, Mundada AS. "Swine Influenza A (H1N1 Virus): A Pandemic Disease." Systematic Reviews in Pharmacy 2.2 (2011), 110-124. Print. doi:10.4103/0975-8453.86300